Engineer

Довела, що блокування вторгнень працює щоразу

Довела працездатність усього ланцюжка блокування вторгнень під час кожного запуску посилення захисту: блокувала зарезервовану тестову адресу, зчитувала створене правило ядра й знімала блокування в гарантованому блоці очищення, тож jail, який перестав працювати, обриває запуск помилкою, а не звітує про справність.

вересень 2026

блокування перевірено під час кожного прогону посилення захисту

Ситуація. Службу блокування зловмисників уже ловили на тому, що вона блокувала порт, на якому демон SSH не слухав. Виправлення порту закрило той конкретний випадок, але ніяк не зачепило причини, з якої помилка проіснувала так довго: збій на шляху блокування нічим себе не виявляє — служба працює, jail значиться активним, і ніщо ніде не показує, чи доходить до ядра хоч одне блокування.

Завдання. Шлях блокування треба було випробовувати під час кожного converge на живому наборі правил, а не робити висновок про його справність лише з того, що служба запущена.

Дія. Тепер converge блокує адресу з діапазону, який стандарти резервують для документації, зчитує з фільтра пакетів ядра правило, що з’явилося, і знімає блокування в блоці очищення, який виконується незалежно від того, пройшла перевірка чи ні. Ключовий вибір тут — зарезервований діапазон: тестова адреса нікому не належить, тож випадкове блокування, яке переживе невдалий прогін, не відріже справжню мережу. Друга половина — зчитування з ядра: власний вивід стану служби повідомив би про успішне блокування, навіть якщо воно не створило жодного правила, а це саме той збій, який і перевіряють. Крім того, механізм блокування закріплено явно, а не залишено на автовизначення службою, а

джерело журналу, навпаки, переведено на автовизначення, бо операційна система не постачає традиційного журналу автентифікації, а за хибного вибору служба мовчки ламається, стежачи за файлом, який ніколи не з'явиться.

Результат. Якщо шлях блокування перестає працювати, converge тепер обривається, а не звітує й далі про справність, — і лише ця властивість насправді мала значення. Це коштує кількох секунд на кожному прогоні, а ще щоразу додає й прибирає правило брандмауера на продакшні — тобто справді втручається в живу систему; на це пішли, бо альтернатива вже довела, що вона гірша.

Застосуйте цей досвід у своєму проєкті

Використайте «Довела, що блокування вторгнень працює щоразу» як відправну точку для схожого завдання у вашій організації. Послуги, що стоять за цією роботою, доступні й для вашого проєкту. Моніторинг і сповіщення, які попереджають, поки збій ще малий, і цифри, що показують, як часто так і залишається.

Переглянути наші послуги Зв'язатися з нами →

Дізнайтеся, що привело до результату

Прочитайте про ситуацію, рішення та результат цього прикладу. Ми можемо обговорити, що відповідає вашим умовам, а що потребує іншого підходу. Довела, що блокування вторгнень працює щоразу — блокування перевірено під час кожного прогону посилення захисту

Переглянути наші послуги Зв'язатися з нами →

Помітили б ви, якби засіб захисту перестав працювати?

Обговоріть свій проєкт з інженером, відповідальним за виконання. Обсяг, основу розрахунку вартості та передачу результатів узгоджуємо письмово до початку робіт.

Роль у цій роботі: Інженер з безпеки. Тут задіяні Інфраструктура, Автоматизація та CI/CD, Надійність і резервне копіювання, Linux та сервери, Безпека та Тестування та QA. І, до речі, ми добре вміємо Надійність та моніторинг (SRE), Системне адміністрування, Безпека та керування доступом та Безпека ШІ-агентів.

Зв'язатися з нами Ознайомтеся з нашими послугами

Одна частина **довшого переліку** — і він увесь на цьому сайті.

Кожен запис написано однаково: ситуація, завдання, що ми зробили і що змінилося.

Переглянути весь перелік

Визначте потрібне покращення

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Помітили б ви, якби засіб захисту перестав працювати?

Запитайте про рішення в роботі «Довела, що блокування вторгнень працює щоразу». Ви говоритимете з людьми, які можуть пояснити роботу й оцінити ваш проєкт.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/portfolio/proved-the-intrusion-ban-works-every-run/