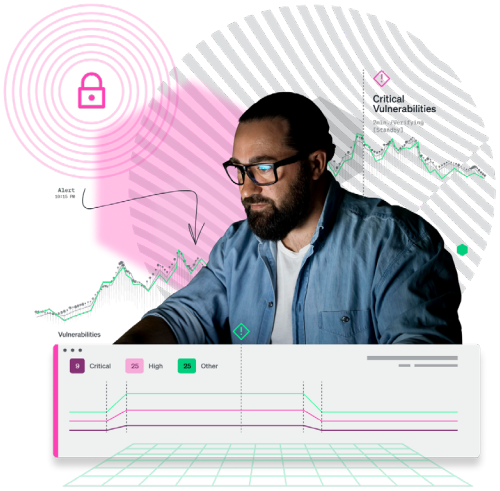
new relic

FICHE TECHNIQUE

Test interactif de sécurité des applications (IAST) New Relic

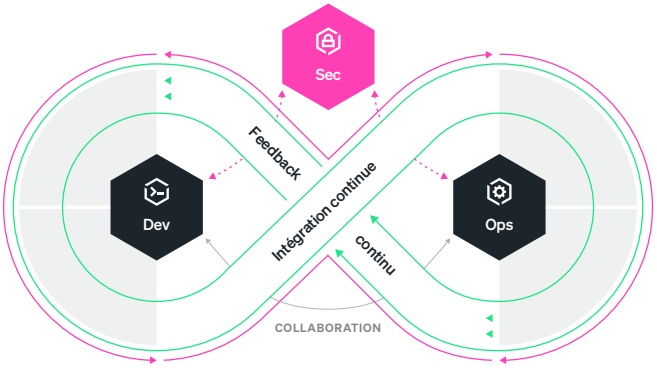
IAST précis, rapide. Envoyez votre code plus rapidement grâce à la précision sans égale de la détection des risques de sécurité.



Les pratiques en termes de tests de sécurité des applications actuelles manquent de précision et de cohérence, ce qui engendre des faux positifs, des cycles de sortie de logiciels manqués et des coûts de sécurité plus élevés. Pour développer des applications plus sécurisées, les équipes DevOps ont besoin d'une solution qui fournisse une visibilité complète sur le cycle de vie des applications, élimine les faux positifs, et facilite la détection et la résolution des risques de sécurité réels.

New Relic IAST va au-delà des approches conventionnelles, en fournissant la visibilité et le contexte nécessaires aux observations de sécurité, une détection d'une précision sans égale, et une preuve d'exploitation grâce à ses capacités d'évaluation dynamiques qui identifient la source des vulnérabilités en simulant des attaques réelles—avec une remédiation guidée pour une résolution plus rapide. De plus, New Relic IAST est entièrement intégrée à la gestion des vulnérabilités New Relic. Vous pouvez ainsi continuer de détecter, corriger et vérifier les vulnérabilités à haut risque tout au long du cycle de développement des logiciels (SDLC).

New Relic IAST, qui fait partie de la plateforme d'observabilité New Relic, permet aux équipes DevOps et de sécurité de monitorer, tester et résoudre précisément et continuellement les risques de sécurité tout au long du SDLC de façon évolutive, et d'envoyer votre code plus vite.



AVANTAGES

Une observation globale pour éliminer les angles morts

Bénéficiez d'une visibilité sur tout votre stack d'applications et les relations associées avec des informations contextuelles pour éliminer les angles morts et valider les efforts de remédiation.

Amélioration de la précision des tests de sécurité

Éliminez les faux positifs grâce à la détection précise et rapide, à la priorisation des risques et à la validation automatisée des vulnérabilités.

Concentration sur ce qui est important avec une validation des exploitations par la preuve

Trouvez, résolvez et vérifiez les vulnérabilités exploitables pour une remédiation plus rapide grâce à des capacités d'évaluation dynamiques qui éliminent la nécessité de changements de code.

Accélération des efforts de remédiation

La remédiation guidée et des garde-corps permettent aux développeurs d'éviter des erreurs critiques en identifiant l'emplacement du code, la trace du stack, la trace HTTP, les URL rencontrées, ainsi que le mécanisme et les paramètres d'exploitation, et plus encore.

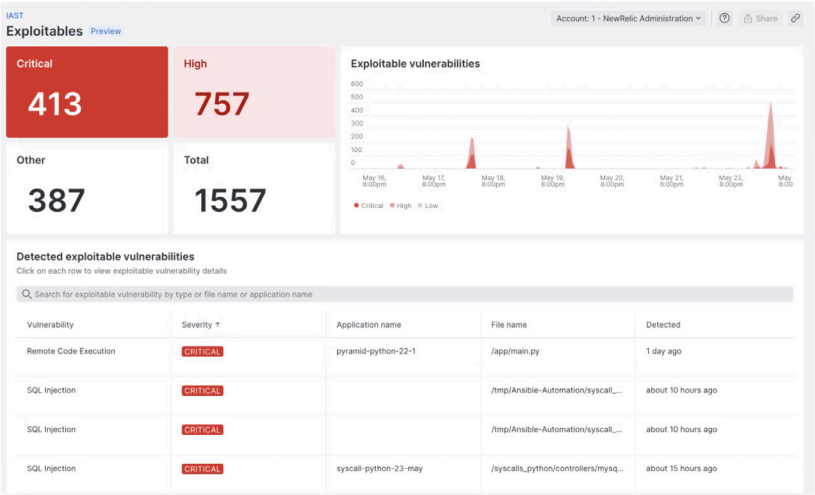
Évolution à volonté

Le déploiement facile via l'agent APM existant, l'intégration fluide aux pipelines d'intégration continue et de livraison continue (CI/CD) et les systèmes de tickets aident à empêcher toute interruption des processus et workflows existants.

CAPACITÉS

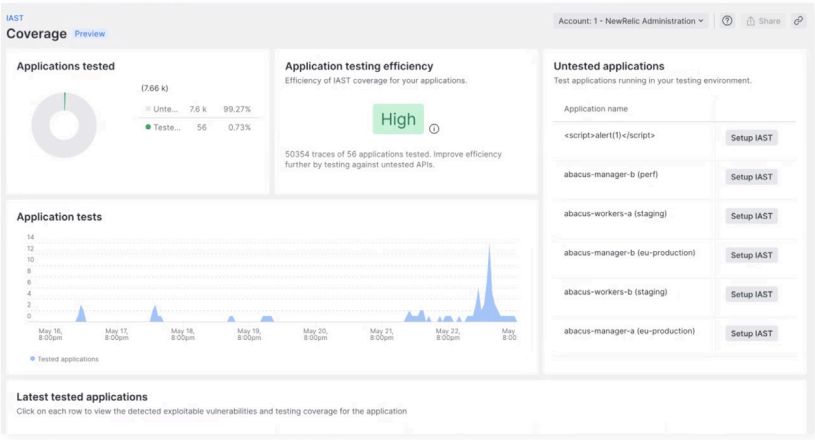
Bénéficiez d'une visibilité sur tout le stack d'applications

Observez toutes les applications protégées et non protégées pour éliminer les angles morts et identifier les menaces cachées, et monitorez et validez le statut des efforts de remédiation afin de faire en sorte que les applications soient toujours protégées.



Mettez le doigt sur l'emplacement exact des vulnérabilités en temps réel avec quasiment aucun faux positif

Identifiez les vulnérabilités dans toutes les couches du stack d'applications et réduisez les faux positifs grâce à une détection rapide et précise, ce qui permettra aux développeurs de se concentrer sur des menaces de sécurité réelles avec des listes de vulnérabilités priorisées selon le risque pour une remédiation plus rapide.

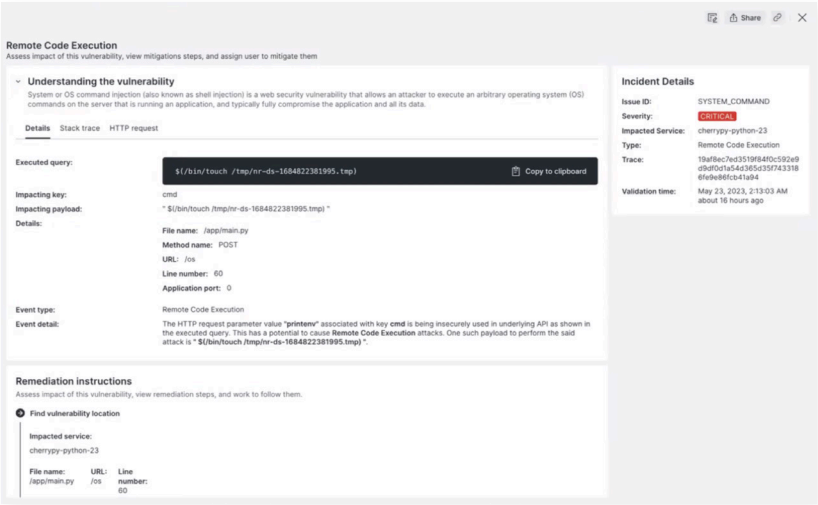


« New Relic IAST permet à notre équipe de développement de coder en toute confiance en automatisant certaines tâches et en lui fournissant une vue complète des risques de sécurité, notamment une rétroaction en temps réel, des informations précises et une analyse de sécurité en contexte. Le tout se fait dans le cadre de nos pratiques d'observabilité sans entraver le processus de développement. »

Agustín Paroli
Directeur des opérations informatiques chez D24

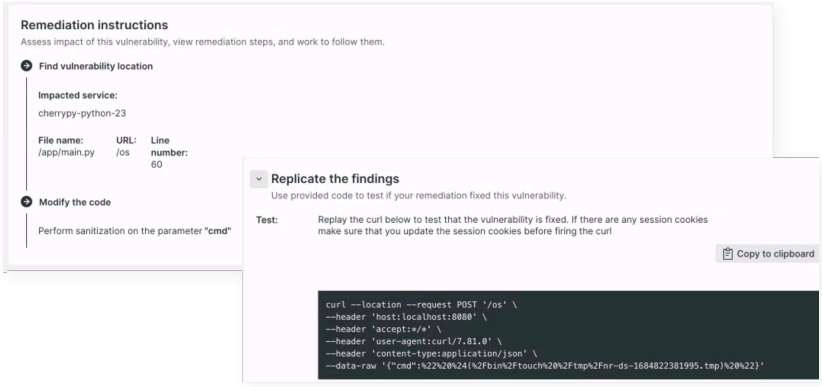
Identifiez les vulnérabilités avec preuve d'exploitation

Gagnez du temps grâce aux capacités d'évaluation dynamiques qui identifient la source des vulnérabilités en simulant des attaques réelles. Validez-les ensuite avec preuve d'exploitation pour permettre aux développeurs de se concentrer sur des vulnérabilités vérifiées et d'envoyer un code plus sûr.



Remédiation guidée pour une élimination efficace et rapide des risques de sécurité

Classez automatiquement les failles de logiciels telles que l'injection SQL, l'exécution de commandes, et d'autres normes dans le Top 10 d'OWASP, puis éliminez-les avant qu'elles ne soient exploitées. Grâce à la remédiation guidée et aux garde-corps des experts New Relic, les développeurs peuvent éviter des erreurs critiques qui pourraient entraîner un incident de sécurité potentiel.



Étapes suivantes

- En savoir plus
- Démarrer
- Contactez-nous

new relic.