# LE GUIDE DU CLIENT SUR LES TESTS D'INTRUSION

**Évitez la confusion :**
**Comment Choisir le Scanner,**
**le Test d'intrusion, Bug Bounty,**
**ou la Plateforme sécurité de**
**testing qu'il vous faut ?**

Synack

## Table des matières

Les infractions sont trop fréquentes aujourd'hui, car les cybercriminels déterminés s'organisent et ciblent mieux avant d'attaquer. Dans de nombreux cas, un cadre d'entreprise perd son emploi à la suite de ces attaques. Ce ne doit pas être vous ou votre entreprise.

Une solution de test efficace est un élément clé de votre sécurité. En recherchant la solution parfaitement adaptée à votre entreprise, assurez-vous de prioriser vos objectifs. Aspirez-vous à la sécurité globale pour réduire les risques d'intrusion? Visez-vous uniquement la conformité? Un client ou un partenaire insiste-t-il afin que vous fassiez un contrôle? Cherchez-vous un test ponctuel ou une sécurité continue en fonction de l'évolution de votre réseau et de vos applications?

Compte tenu de ces objectifs, vous pourrez tirer le meilleur parti des informations présentées dans ce guide. Mais avant d'étudier de près des solutions alternatives et des spécificités du testing, commençons par une mise en contexte.

## La genèse des tests de sécurité

Les tests d'intrusion existent depuis le début des années 1970. Ils se font plus courants à mesure que les systèmes et services informatiques évoluent et deviennent une partie cruciale des opérations métiers. Les organisations font appel à des spécialistes capables d'analyser les tactiques, techniques et procédures (TTP) des agresseurs potentiels. Ce test fournit une évaluation précise, objective des réseaux et des systèmes de sécurité.

Cependant, les environnements numériques deviennent de plus en plus étendus, ainsi que leurs surfaces d'attaque. Si les humains sont créatifs, nous avons des limites. Les scanners sont apparus à la fin des années 1990 pour donner une échelle supplémentaire et une certaine profondeur aux tests de sécurité. Finalement, le besoin de talent et de rigueur supplémentaires pour trouver et corriger les vulnérabilités de manière proactive a donné naissance aux tests de sécurité collaboratifs au début des années 2000.

### LES AVANTAGES DU TEST D'INTRUSION

- **L'adhésion des dirigeants**—28% des vulnérabilités découvertes sont très graves.[1] Cela signifie qu'en l'absence de tests et de mesures correctives, le risque d'intrusion est important. C'est un sujet qui préoccupe les dirigeants.
- **Des données exploitables**—Pour être utile, chaque vulnérabilité découverte doit être validée avec des étapes explicites à reproduire, donnant aux clients la possibilité d'y remédier rapidement.
- **La réduction des risques de vulnérabilité**—Les entreprises deviennent plus sécurisées, puisque la détection et la réduction des vulnérabilités permettent d'atténuer les risques d'intrusion.
- **L'évaluation objective**—Les meilleures pratiques de l'industrie sont mises à profit pour sécuriser votre entreprise en utilisant des règlements et des critères de conformité lors d'un test de sécurité.

## La stratégie sécurité efficace

La sécurité efficace signifie à la fois la protection des actifs de valeur élevée et l'augmenation du niveau de sécurité au sein de l'entreprise. En 2019, plus de 17 000 vulnérabilités ont été signalées aux États-Unis (et le nombre total de vulnérabilités découvertes est probablement beaucoup plus élevé).[2] Pour être en sécurité, les entreprises doivent trouver et corriger chaque vulnérabilité critique dans tous les systèmes importants, car un attaquant n'a besoin que d'une seule pour réussir.

## Qu'entendons-nous par profondeur et étendue des tests?

Les tests d'intrusion ont encore évolué pour suivre les cycles continus de développement de logiciels et le besoin constant d'informations de qualité sur la sécurité.

**PROFONDEUR**

*Les criminels se concentrent parfois sur un actif particulier et effectuent de nombreuses attaques en plusieurs étapes pour y accéder. Des tests en profondeur peuvent atténuer ce genre d'attaques.*

**ÉTENDUE**

*Les attaquants utilisent souvent des "bots" automatisés pour trouver des moyens faciles d'accéder à un réseau ou actif. Des tests étendus (mais superficiels) à l'aide de scanners peuvent remédier à ce genre de vulnérabilités.*

1 Les données de Synack Red Team, période de 12 mois précédant le 1 janvier 2020.

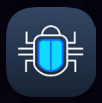
2 La Base de données nationale sur les vulnérabilités, https://nvd.nist.gov/vuln/search.

## Les types de tests de sécurité

Les tests de sécurité se répartissent en quatre catégories de base :

**le balayage** à l'aide de logiciels pour rechercher des systèmes vulnérables ou non autorisés et des services [à la machine]

**le test d'intrusion traditionnel** qui implique l'évaluation des vulnérabilités communes, en s'appuyant sur le Open Web Application Security Project (OWASP) ou autre organisme de normalisation [réalisé par un consultant].



**le test basé sur le modèle Bug Bounty** les chercheurs sont autorisés à s'attaquer à l'actif de manière créative et sont motivés par des primes [activité collaborative].

**la plateforme sécurité de test collaboratif** qui combine les meilleurs éléments des trois catégories ci-dessus - il s'agit de la prochaine génération de pentesting [la plateforme et l'expertise humaine].

## Le balayage

Les scanners sont utilisés pour couvrir une large surface d'attaque contre des actifs à faible risque. Bien que les scanners ne permettent pas d'effectuer des tests de sécurité profonds comme c'est le cas dans la sécurisation globale (les scanners ne peuvent pas simuler des attaques en plusieurs étapes ni offrir la créativité des chercheurs), ils donnent une mesure "large mais peu profonde" de la résistance aux vulnérabilités connues. Parmi les acteurs de cette catégorie, on peut citer Tenable, Rapid7, WhiteHat et Qualys.[3]

Si les scanners sont omniprésents et peu coûteux, ils présentent certaines limites fondamentales lorsqu'ils sont utilisés comme des solutions autonomes. Par exemple, les actifs de valeur élevée nécessiteront presque toujours un certain niveau d'interaction humaine. Les scanners ne sont pas non plus capables de réaliser des exploits complexes en plusieurs étapes ou zéro jour comme le font les chercheurs. Pour ces raisons, bien que les scanners restent un élément essentiel du testing de sécurité, ils ne sont pas considérés comme suffisants pour fournir une évaluation réaliste du risque de sécurité.

3 Gartner Magic Quadrant for Application Security Testing, Horvath, Zumerle, et Gardner, ID G00394281 29 Avril, 2020

## Le test d'intrusion traditionnel (basé sur les listes de contrôle)

Ce qui était autrefois un "pentest" a beaucoup changé au fil des ans. Le test d'intrusion traditionnel a été conçu pour fournir la meilleure qualité de testing créatif, principalement manuel et fait à un moment précis. Récemment, le terme "pentest" (surtout dans le secteur privé) a été cependant remplacé par une version plus réduite de lui-même, qui consiste souvent à effectuer des tests uniquement à l'aide d'une liste de contrôle. Dans la majeure partie de ce document, nous ferons référence au "test d'intrusion traditionnel" pour désigner la version "réduite" plus actuelle. La majorité des équipes de pentesting sont composées d'une ou deux personnes.

Les quatre grands cabinets de conseil (Deloitte, E&Y, PwC, KPMG) sont de bons exemples de cette catégorie. Parmi les acteurs plus spécialisés, citons NCC Group, Bishop Fox et Cipher. Enfin, il existe une multitude de petites sociétés régionales indépendantes (également appelées "boutiques de conseil") qui utilisent ce procédé.

L'efficacité de cette méthode dépend de la profondeur de l'évaluation dont une entreprise a besoin et du talent des testeurs dont dispose le fournisseur. Les avantages de cette méthode sont notamment sa simplicité et sa portée limitée. Les inconvénients sont les suivants: pas de concurrence entre les testeurs, pas d'incitation à la créativité, un ensemble de compétences très limité pour chaque vulnérabilité, pas d'informations en temps réel sur les résultats et des remédiations tardives.

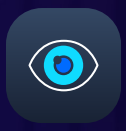
## Le test basé sur le modèle Bug Bounty

Les tests de sécurité basés sur le modèle Bug Bounty exploitent un ensemble varié de compétences en testing, utilisant un modèle de récompense pour inciter les chercheurs à imiter le comportement de l'adversaire. Cela leur permet d'évaluer la sécurité globale plutôt que de simplement faire des contrôles de sécurité prédéfinis. Ce faisant, ils peuvent également combler les lacunes où les tests d'intrusion traditionnels échouent. Plusieurs sous-catégories sont concernées par ce regroupement (voir plus de détails à la page suivante). Parmi les acteurs de cet espace figurent Cobalt, Bugcrowd et HackerOne. Plusieurs entreprises mentionnées préferent effectuer des tests à l'aide des listes de contrôle pour leur large clientèle et réservent la véritable méthode de crowdsourcing à leurs grandes entreprises clientes; mais elles sont classées ici par souci de simplicité.

L'avantage des tests de sécurité basés sur le Bug Bounty consiste à un modèle de récompense incitant les chercheurs à détecter plus de vulnérabilités que ne le ferait le test d'intrusion traditionnel. Un plus vaste éventail de chercheurs et de compétences (souvent plus de 50 chercheurs postulent pour un test), ainsi que la concurrence assurent une meilleure performance globale et une évaluation plus approfondie. Cette catégorie est plus complexe et offre différents niveaux de contrôle. Une bonne décision d'achat exige du discernement de la part de l'acheteur. (Voir la page suivante pour plus de détails sur les avantages et les inconvénients).

# Les informations concernant les tests basés sur le modèle Bug Bounty

Bien qu'ils soient regroupés dans la même catégorie, il existe différents types de récompenses et de tests de sécurité collaboratifs, dont certains sont plus efficaces que d'autres :



**VULNERABILITY DISCLOSURE PROGRAMS** (VDP, aussi appelés Responsible Disclosure Programs) : Bien qu'il ne s'agisse pas techniquement d'une récompense Bug Bounty (il n'y a pas de prime réelle), il s'agit d'une politique "voir quelque chose, signaler quelque chose" dans laquelle une entreprise fait appel à un fournisseur pour gérer un programme où n'importe qui peut signaler la découverte d'une vulnérabilité.

**Advantages:** peu coûteux, assez simple à mettre en œuvre, une participation publique positive.

**Inconvénients:** des charges opérationnelles potentielles à cause de multiples rapports de mauvaise qualité; un manque de contrôle, puisque la vulnérabilité peut être soumise par n'importe qui et certains auteurs s'estimeront en droit d'informer le public si vous ne répondez pas dans un certain délai.

**LE MARCHÉ DE BUG BOUNTY:** une somme d'argent est proposé aux chercheurs qui tentent de pirater les actifs informatiques d'entreprise. Ce système est similaire au VDP, sauf qu'il y a une récompense pour la découverte de vulnérabilités. Dans certains cas, le programme de récompense Bug Bounty n'est accessible qu'à un groupe spécifique de pirates éthiques (appelés aussi chercheurs en sécurité).

**Advantages:** la nature compétitive permet d'obtenir de meilleures performances; la diversité des compétences et l'expérience mises à profit pour effectuer des tests.

**Inconvénients:** un contrôle limité et un risque potentiel si la communauté de chercheurs n'est pas gérée; des charges opérationnelles potentielles à cause de multiples rapports de qualité variable.

**LE MICRO-CROWDSOURCING:** Certaines entreprises prétendent réaliser du "crowdsourcing" ou du "bug bounty". Mais en fait, il s'agit d'un nombre limité (une ou deux personnes) de chercheurs qui sont souvent directement rémunérés plutôt que motivés par le modèle de récompense Bug Bounty et qui suivent généralement des listes de contrôle.

**Advantages:** peu coûteux et relativement rapide (bien que ce soit quelque peu trompeur)

**Inconvénients:** même si le terme "crowdsourcing" donne l'illusion d'un testing collaboratif, le petit nombre de chercheurs et l'absence de concurrence le rendent moins efficace qu'un véritable crowdsourcing. Cela appartient en fait à la catégorie des "tests d'intrusion traditionnels".

# Approche des Plateformes sécurité de tests d'intrusion collaboratifs

## Combiner les éléments essentiels d'un test de sécurité

La solution de test la plus robuste - la plateforme sécurité de test "crowdsourced " - associe la créativité et l'ingéniosité de la découverte collaborative de vulnérabilités, l'approche méthodologique des tests d'intrusion à l'extensibilité et la couverture d'un scanner haut de gamme. Cela permet aux entreprises d'effectuer des tests d'intrusion ciblés, de découvrir des vulnérabilités inconnues et de recueillir de nouveaux renseignements de manière évolutive. Ces renseignements sont ensuite transmis dans le système de balayage qui combine l'AI et le talent humain, ce qui permet d'analyser les vulnérabilités suspectes. La plateforme identifie les sources de risque des actifs sur une couverture d'attaque évolutive et globale afin que l'équipe de recherche puisse enquêter.

La plateforme sécurité de test collaboratif transforme tous ces éléments en un processus de test d'intrusion continu et permanent, avec une coordination bien orchestrée entre les chercheurs, le scanner et les activités de conformité. Elle réunit le travail des experts en sécurité et des scanners intelligents (AI/ML), ainsi que le flux de travail bien géré pour assurer le testing collaboratif. On peut aussi dire que les trois composantes ci-dessus sont intégrées et gérées par une plateforme intelligente pour tirer le meilleur de chaque modalité. En fait, Synack est le seul représentant de cette catégorie, bien que de nombreux fournisseurs utilisant le modèle bug bounty prétendent l'être.

Les chercheurs et les technologies intelligentes travaillent ensemble grâce à une plateforme intégrée qui coordonne leurs interactions; ils se complètent pour offrir à la fois des informations pertinentes et une couverture continue. Grâce à la précision qui découle de l'orchestration intelligente de l'application, au lieu de plafonner la récompense, le fournisseur assume la responsabilité du coût total des tests, et toutes les vulnérabilités importantes sont portées à votre attention.

> *Nous avons découvert le produit de Synack comme le plus professionnel, réactif, performant et mieux conçu.*
>
> **PDG ET CO-FONDATEUR,**
> **SOCIÉTÉ FINANCIÈRE INTERNATIONALE**

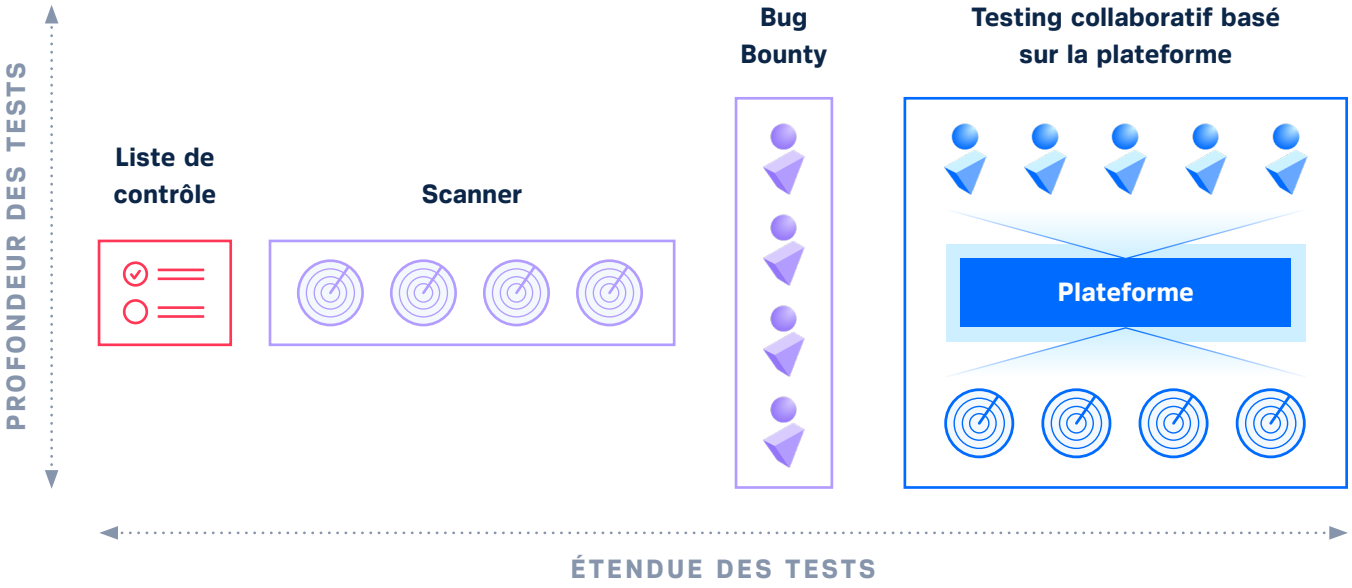
## Quels sont les avantages des plateformes sécurité de test collaboratif?

- Le balayage assure une vaste couverture des actifs à faible risque
- L'AI/ML orchestre l'effort humain
- Le test d'intrusion continu, 24 heures sur 24, 7 jours sur 7, 365 jours par an
- L'ingéniosité des chercheurs se concentre sur les actifs à haut risque
- Les chercheurs apportent leurs vastes compétences, créativité et TTP au processus de découverte
- Contrairement au modèle Bug Bounty traditionnel, il n'y a pas de plafonnement des récompenses
- Vous contrôlez le testing (mettre en pause et démarrer, protéger les actifs par une passerelle sécurisée) du début à la fin
- La plateforme fournit des résultats et des analyses exploitables et en temps réel

## Les caractéristiques par catégorie

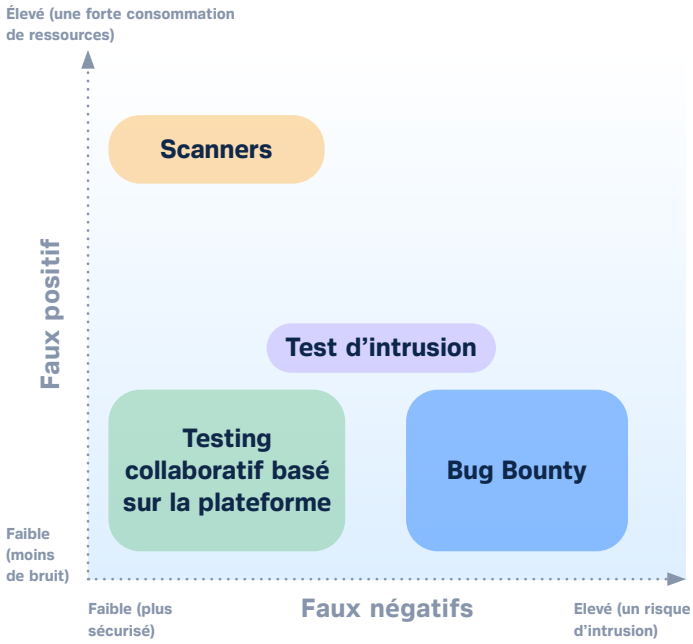
| ✓ Bon<br>✗ Mauvais | Scanner | Test d'intrusion traditionnel (liste de contrôle) | Test basé sur le modèle Bug Bounty | Plateforme sécurité de test collaboratif |
|---|---|---|---|---|
| **Value (coverage/ cost)** | ✓ | ✓ | ✓ Pour certains actifs spécifiques | ✓ |
| **Security/Trust of Process** | ✓ | ✓ | ✗ | ✓ |
| **Scalability (across full attack surface)** | ✓ | ✗ | ✗ Actifs de grande valeur uniquement | ✓ |
| **Test Accuracy (quality of vulns)** | ✗ Faux positifs | ✗ Faux négatifs | ✗ Certaines catégories hyper-profondes; d'autres totalement absentes | ✓ |
| **Full Service Support** | ✗ | ✗ | ✗ | ✓ |

### COMPARAISON DES DIFFÉRENTES MÉTHODES DE TEST DE SÉCURITÉ




## Quel est le retour sur investissement des tests d'intrusion?

En fin de compte, la technique de crowdsourcing basée sur la plateforme assure un retour sur investissement quatre fois plus élevé que le test d'intrusion traditionnel. Sur le plan quantitatif, cela représente un retour sur investissement de 159 % grâce à une efficacité, efficience et échelle accrues.[4]




4 L'estimation du retour sur investissement est basée sur les données de Synack jusqu'au premier trimestre 2020. Cela suppose une comparaison avec un test d'intrusion traditionnel coûtant 30 000 $ pour 80 heures de test, 6 semaines pour démarrer avec un nouveau client et 1 semaine de travail pour la génération de rapports

## LE RETOUR SUR INVESTISSEMENT DE LA PLATEFORME SÉCURITÉ DE TEST COLLABORATIF

**159 %**

**de retour sur investissement, soit 4 fois plus que les tests d'intrusion traditionnels**

**3x**

**plus de temps passé sur la cible par rapport aux tests d'intrusion traditionnels**

**20%**

**Réduction de 20 % des correctifs échoués grâce au processus de Patch Verification**

**<72 h**

**de recrutement des experts contre des semaines dans le modèle traditionnel**

## Pourquoi Synack utilise une plateforme sécurisée et fiable

La confiance est la clé des solutions de crowdsourcing. Si les risques au sein de la communauté (concernant la communication des vulnérabilités au public) ne sont pas maîtrisés, les entreprises peuvent se retrouver engagées dans un processus de fuite à cause des vulnérabilités découvertes plus vite que les responsables ne puissent y remédier; beaucoup de résultats bruyants sans un signal clair; et/ou des chercheurs menaçant de divulguer les vulnérabilités si elles ne sont pas corrigées dans un certain délai.

### ATTENTION AUX MINES

- **La sous-traitance d'un tiers pour les tests d'intrusion**—Souvent, le principal fournisseur des solutions de sécurité sous-traite un service de pentesting pour améliorer son offre; ou, dans certains cas, il s'agit de plusieurs chercheurs afin d'obtenir une équipe de recherche plus diversifiée. Le problème est qu'il n'y a pas de responsabilité claire dans ces scénarios, ce qui mène souvent à des accusations et à une mauvaise coordination entre les sociétés.
- **Les faux tests d'intrusion**—De nombreuses entreprises prétendant utiliser une communauté de chercheurs engagent en fait 1 à 3 chercheurs dans votre projet. Cela n'apporte pas suffisamment d'ampleur ni de profondeur au testing. C'est ce que l'on appelle "Deux testeurs, deux ordinateurs portables, deux semaines".
- **L'absence de concurrence entre les chercheurs**—Une communauté peu nombreuse ne peut guère cultiver un environnement compétitif. Lors de véritables tests d'intrusion, les chercheurs agissent indépendamment et le premier qui trouve et documente la vulnérabilité – de façon plus rapide et approfondie - est rémunéré. Imaginez à quoi ressemblerait un match de boxe avec un seul boxeur.
- **La liste de contrôle de Bug Bounty**—En raison de la popularité du crowdsourcing, certaines organisations confondent ce concept collaboratif basé sur les récompenses avec un modèle de liste de contrôle simple. Les deux méthodes sont importantes en matière de sécurité, mais ne vous laissez pas tromper en pensant qu'une liste de contrôle remplace les tests de sécurité collaboratifs.
- **L'analyse manuelle**—En matière d'analyse, il ne faut pas oublier le principe GIGO (garbage in, garbage out). Pour que les analyses soient exploitables, elles doivent s'appuyer sur des données fiables. Certaines plateformes utilisent des analyses basées sur des processus manuels ou des évaluations humaines, plutôt que des algorithmes solides et objectifs, ce qui les rend peu fiables.
- **L'illusion de contrôle**—De nombreuses plateformes sécurité de tests collaboratifs prétendent assurer le contrôle client du processus de crowdsourcing. En outre, le "contrôle" des chercheurs est devenu approximatif. Les clients devraient demander au fournisseur comment il contrôle sa communauté de chercheurs et s'il surveille en permanence leur activité. Les clients veulent avoir une visibilité 24 heures sur 24, 7 jours sur 7 et 365 jours par an des tests au sein de la plateforme, y compris la possibilité de mettre en pause et de redémarrer le processus.
- **L'absence de vérification des correctifs**—Méfiez-vous des entreprises qui ne fournissent pas de tests de vérification des patches. Environ un tiers des correctifs initiaux échouent. Sans un nouveau test, vous ne pouvez pas être sûr que le correctif fonctionne. La seule façon de s'en assurer est de le confirmer par un test de vérification.

Synack aborde cette question de deux manières. Premièrement, nous contrôlons chaque candidature pour s'assurer que seulement les chercheurs professionnels et éthiques sont recrutés dans l'équipe Red de Synack - en plus de prouver leurs compétences et expérience haut de gamme. Deuxièmement, tous les tests sont effectués par une passerelle sécurisée et gérés par notre plateforme. Cela nous permet de surveiller et de contrôler en permanence les activités des chercheurs et leur comportement afin de nous assurer qu'ils répondent à nos normes élevées. Enfin, pour garantir une protection maximale et le respect de la vie privée, nous fournissons des environnements sécurisés et virtualisés pour nos chercheurs. La plus grande confidentialité des données est assurée grâce à un contrôle total des terminaux que Synack effectue.

> *Ils engagent de nombreux chercheurs bien expérimentés et compétents. On ne paie pas plus pour avoir plus de chercheurs... Je suis heureux de pouvoir dire que nos attentes ont été dépassées.*
>
> **ANALYSTE PRINCIPAL DE LA SÉCURITÉ CLOUD DANS LE SECTEUR DES SERVICES**

## Analyse des produits de Synack

Le tableau suivant vous donne un aperçu général des caractéristiques haut niveau et de leur intégration dans les différentes offres. Cela permettrait de mettre en contexte les caractéristiques clés et leur valeur respective.

| | **Découvrir :** Découverte collaborative des vulnérabilités | **Certifier :** Test d'intrusion collaboratif | **Synack365:** Test d'intrusion collaboratif continue |
|---|---|---|---|
| **Durée** | Limité dans le temps | En continu | En continu |
| **Plateforme intelligente, avec des résultats et des analyses en temps réel** | ✓ | ✓ | ✓ |
| **Programme de divulgation des vulnérabilités (VDP)** | ✓ Inclus avec l'achat de quatre tests ou plus | ✓ | ✓ |
| **Chasse aux vulnérabilités motivée par le modèle de récompense** | ✓ | ✓ | ✓ |
| **SmartScan avec triage** | ✓ | ✓ | ✓ |
| **Test basé sur la méthodologie (liste de contrôle)** | | ✓ | ✓ |
| **Couverture des tests 365 par l'équipe Red de Synack** | | | ✓ |

## Conclusion

Les scanners autonomes vous fourniront une couverture large (mais superficielle) de la surface d'attaque pour les actifs de faible valeur. Le test d'intrusion traditionnel donne une vision superficielle de certains actifs, mais il n'est pas évolutif, a une faible traçabilité et manque d'analyse. Le test de sécurité de type "bug bounty" offre une analyse plus profonde d'un ou de plusieurs actifs précieux.

Toutefois, c'est la plateforme de crowdsourcing qui représente la prochaine génération de tests de sécurité fiables et globales, en assurant l'étendue et la profondeur des évaluations. Elle combine l'évolutivité, le talent et l'expertise humains, avec la large couverture d'un scanner et l'exigence de conformité d'une liste de contrôle. La plateforme de tests collaboratifs vous offre une couverture approfondie tout au long de l'année. Ce n'est qu'avec une équipe de chercheurs contrôlés et une plateforme intelligente et continue que vous obtiendrez une couverture de sécurité complète, ainsi qu'un réel retour sur investissement.

> *Les tests de sécurité sont devenus une priorité pour chaque PDG et ingénieur en sécurité. Le coût global des cybercrimes devrait atteindre 6T$ d'ici 2021. Les organisations ne peuvent tout simplement pas embaucher les talents dont elles ont besoin pour faire face à cette menace, ni compter sur des défenses archaïques. Pour minimiser les risques de sécurité, les entreprises ont besoin de plateformes de test de sécurité évolutives et complètes, optimisées tant en profondeur qu'en étendue, sans compromis.*
>
> **—B CAPITAL GROUP**

# Annexe A : Checklist pour sélectionner un fournisseur en tests d'intrusion

Pour choisir entre le test d'intrusion traditionnel,  Bug Bounty et la plateforme de test collaboratif, cette liste de contrôle peut vous aider à évaluer les fournisseurs.

| | Le fournisseur a: |
|---|---|
| **Chercheurs** | |
| Des centaines de testeurs disponibles (environ 50-80 par test) pour garantir l'étendue et la profondeur des compétences et de l'expérience | ○ |
| Une communauté de chercheurs pleinement contrôlés - y compris des tests de compétences, des entretiens et des vérifications d'antécédents - pour garantir la sécurité et la qualité | ○ |
| Un modèle basé sur des récompenses pour encourager l'ingéniosité et l'esprit compétitif | ○ |
| Des chercheurs qui sont à la demande et indépendants plutôt que salariés, qui mettent leurs compétences au service de votre sécurité, si nécessaire | ○ |
| **Protection et Confiance** | |
| Le client n'est pas responsable des activités futures des chercheurs | ○ |
| Le client est propriétaire des données et de l'IP de la vulnérabilité détectée (pas le fournisseur ni le chercheur) | ○ |
| L'analyse de la couverture, quand/quoi/comment (c'est-à-dire les tentatives d'attaque) les applications et les actifs en question ont été évalués à la suite des activités des chercheurs | ○ |
| Les paiements sont gérés par le fournisseur pour protéger le client | ○ |
| Pas d'exception de "dernier recours" au domaine privé pour signaler les vulnérabilités | ○ |
| Le démarrage, arrêt et reprise des fonctions contrôlés par le client pendant les tests | ○ |
| **Technologie** | |
| Une analyse automatisée des vulnérabilités qui renforce l'activité des chercheurs | ○ |
| Un portail SaaS centralisé qui donne aux clients une visibilité 24 heures sur 24, 7 jours sur 7, 52 semaines sur 52 de leurs tests, résultats, mesures et rapports | ○ |
| La coordination/triage des chercheurs grâce à une plateforme d'orchestration intelligente | ○ |
| Une passerelle sécurisée par laquelle tous les tests sont effectués | ○ |

| | |
|---|---|
| **Processus de découverte de la vulnérabilité** | |
| Des tests de conformité, basés sur une méthodologie, qui vérifient les faiblesses connues | ○ |
| Un modèle incitatif de découverte de la vulnérabilité | ○ |
| Répond aux mandats d'audit et de conformité, tels que PCI, NIST | ○ |
| La suppression des doublons | ○ |
| Une piste de vérification et des mises à jour en temps réel de toutes les activités de recherche | ○ |
| Le nombre de chercheurs, d'heures de recherche enregistrés pour le suivi et la responsabilité | ○ |
| La capacité à communiquer directement avec les chercheurs | ○ |
| **Sécurité efficace** | |
| L'évaluation de l'efficacité des correctifs pour suivre les progrès | ○ |
| Un service de vérification des correctifs entièrement géré avec des récompenses garanties | ○ |
| Le processus de Patch Verification sans risque : la demande de vérification est envoyée uniquement au déclarant | ○ |
| **Rapports et Notation** | |
| Des rapports professionnels, vérifiables, personnalisables (PDF) sur demande | ○ |
| Une analyse humaine du rapport final | ○ |
| La notation claire et objective du renforcement des actifs | ○ |
| Des résultats comparatifs pour suivre les progrès dans le temps et se comparer à ses pairs du secteur | ○ |
| **Plateforme logicielle pour les chercheurs en sécurité** | |
| Un flux de travail à toute épreuve, du scan à la mission, au triage, puis à la vérification des correctifs | ○ |
| Des techniques de détection uniques pour l'hôte, le web, le mobile | ○ |
| Un flux de travail pour l'évaluation de l'exploitabilité en temps réel | ○ |
| **Réduction du bruit et Rationalisation du service client** | |
| Des instructions détaillées sur la remédiation directement rédigées par les chercheurs | ○ |
| Le triage complet de chaque vulnérabilité soumise | ○ |
| Un chef de projet sécurité dédié | ○ |

# Annexe B : Caractéristiques et avantages de la plateforme sécurité de testing collaboratif

La plateforme sécurité de testing collaboratif a de nombreux avantages par rapport à une évaluation traditionnelle.

| CARACTÉRISTIQUES | AVANTAGES |
|---|---|
| **Notation** | Alors qu'une simple liste de vulnérabilités ne contient pas d'informations sur les risques, la notation des vulnérabilités est très importante. Synack utilise la mesure ARS (Attacker Resistance Score), qui quantifie des facteurs variables telles que la difficulté de détection d'une vulnérabilité, sa gravité et l'efficacité avec laquelle elle peut être corrigée. |
| **Aperçu axé sur les données** | Il est essentiel que les informations parviennent aux personnes concernées (qui en ont besoin). Synack fournit des données sur les vulnérabilités aux chercheurs, leur permettant de prendre des décisions éclairées et de trouver des vulnérabilités plus rapidement. Cela vous permettra d'obtenir les informations les plus précises pour évaluer vos risques. |
| **Détection de schémas** | Le balayage et les tests continus mettent en évidence les changements dans une surface d'attaque et les zones de risque potentiel. La connaissance de ces tendances peut être très utile à une entreprise. Cela sert à déterminer si elle subit une attaque ciblée ou si ses politiques ou procédures organisationnelles sont insuffisantes pour répondre aux besoins de sécurité. |
| **Étendue des compétences** | Certaines grandes sociétés de conseil engagent souvent des équipes qui se limitent à une personne pour un test d'intrusion. Cela se traduit par une nombre limité de compétences techniques et d'outils utilisés pour découvrir les failles de sécurité. La véritable méthode de crowdsourcing de Synack n'offre pas seulement de très nombreuses compétences. Notre processus de sélection et de contrôle vous permet d'utiliser les talents et l'intégrité des meilleurs chercheurs. |
| **Sécurité (vs Conformité)** | Les contrôles de conformité ne contribuent guère à une véritable sécurité. La combinaison d'une liste de contrôle de conformité avec des tests collaboratifs basés sur des récompenses ET des missions continues orchestrées par une plateforme intelligente vous met en conformité ET en sécurité |
| **Résultats et Incitations** | Dans les tests d'intrusion traditionnels, les engagements sont basés sur le temps et le matériel. Cela signifie que la société de conseil est payée quel que soit le nombre de failles de sécurité découvertes, exploitées et signalées. La méthode de Synack ne récompense que les vulnérabilités et les exploits confirmés. Les clients sont ainsi assurés de payer pour une valeur réelle et non pas seulement pour le temps passé durant la mission. |

| CARACTÉRISTIQUES | AVANTAGES |
| --- | --- |
| **Validation des vulnérabilités remédiées** | Les tests d'intrusion traditionnels ne permettent pas toujours de vérifier que les failles ont été corrigées. Au lieu de cela, on laisse au client le soin d'effectuer la remédiation et de valider son efficacité par lui-même. Sur le plan procédural, Synack veille non seulement à ce que les étapes de reproduction soient clairement définies, mais aussi à ce que les exploits précédemment démontrés ne soient plus efficaces, évitant ainsi le syndrome du patch raté. Les chercheurs qui découvrent et rapportent des exploits réussis ont des récompenses supplémentaires pour vérifier que ces exploits ont été résolus. |
| **Pistes de vérification** | Les informations consernant le processus de testing ne sont pas capturées par tous les tests. Pour la conformité et les meilleures pratiques de sécurité, Synack utilise à la fois les pistes de vérification et les contrôles techniques en les mettant entièrement à la disposition des clients. |
| **Bouton de démarrage/arrêt pour les tests** | Avoir le contrôle du processus de testing est plus important que vous ne l'imaginez. Il pourrait y avoir un audit inattendue qui nécessiterait un arrêt des tests afin d'éviter des problèmes embarrassants. Synack a mis en place une plateforme sécurisée, vérifiée et flexible qui non seulement met une communauté d'experts à votre service, mais la garde également sous votre contrôle. Elle comprend un bouton "stop/start" qui vous permet de contrôler quand les tests s'arrêtent et redémarrent. |
| **Appropriation des vulnérabilités détectées et Propriété intellectuelle** | Une fois que vous avez effectué des tests et pris des mesures correctives, le facteur le plus important est de contrôler les données sur les vulnérabilités. Certains contrats autorisent la divulgation publique de ces derniers après un certain temps, quel que soit le niveau d'atténuation. Synack donne toujours la propriété intellectuelle et celle des vulnérabilités découvertes au client. |
| **Plateforme intelligente** | Un pentest vraiment efficace nécessite trois composantes principales. Tout d'abord, vous avez besoin d'un groupe de chercheurs hautement qualifiés, ayant des compétences et des outils variés. Ensuite, il faut une technologie de balayage intelligente afin d'accélérer le processus de découverte des vulnérabilités. Enfin, vous avez besoin d'une plateforme sur laquelle les chercheurs peuvent travailler (où vous pouvez suivre et contrôler leurs activités, et grâce à laquelle vous pouvez visualiser les résultats). Cela vous donne des possibilités inégalés et des compétences contrôlables pour bénéficier de la qualité et maîtriser les risques. |

## Annexe C: Glossaire

**Modèle Black Box**—Un test d'intrusion en mode boîte noire détermine les vulnérabilités exploitables d'un système sans authentification. Le chercheur n'a aucune connaissance interne du système cible, ni de son architecture, code source, etc.

**Blue Team**—Des équipes internes conçues pour défendre leur entreprise contre des attaquants du monde réel en comprenant leurs TTP et en faisant évoluer les défenses de l'entreprise en analysant le comportement de l'adversaire.

**Modèle Bug Bounty**—Un modèle de rémunération en fonction des résultats où un montant d'argent est fourni pour inciter les chercheurs à trouver des vulnérabilités. En général, lorsque ce montant a disparu, le test est terminé. Ces tests sont moins axés sur le processus de testing complet et la sécurité, mais servent davantage de point de départ pour renforcer votre environnement.

**Liste de contrôle de conformité**—Une liste de contrôle spécifique (comme l'OWASP, le NIST 800-53 ou le PCI) est utilisée comme guide pour les chercheurs afin de détecter des vulnérabilités spécifiques en contrôlant la conformité et le respect des normes d'audit spécifiques. Cette méthode permet de vérifier efficacement la conformité, mais pas la sécurité totale.

**Test continu**—La couverture 24 heures sur 24, 7 jours sur 7, 365 jours par an. Il peut s'agir d'un engagement annuel sur abonnement qui comprend un scanner et/ou un service entièrement géré avec vérification régulière de la conformité, gestionnaire de programme dédié, services de cadrage, triage des vulnérabilités, alertes, vérification des correctifs, gestion du programme de divulgation des vulnérabilités, analyses et rapports détaillés des données. L'objectif est de réduire et/ou d'éliminer la durée de vie des vulnérabilités exploitables, et d'augmenter continuellement la résistance des systèmes aux cyberattaques.

**Découverte collaborative des vulnérabilités**—Un modèle de test qui incite une communauté de chercheurs à se faire concurrence pour trouver des vulnérabilités. En général, cela peut impliquer de 50 à 100 chercheurs ayant des compétences et une expérience variées et utilisant de nombreuses tactiques, techniques et procédures différentes.

**Modèle Gray Box**—Les testeurs ont généralement une certaine connaissance des éléments internes d'un réseau, y compris éventuellement la documentation sur la conception et l'architecture et un compte interne dans le réseau, ce qui permet une évaluation plus ciblée de la sécurité réseau que celle en boîte noire.

**Test des actifs internes**—simule un attaquant qui tente d'accéder à un actif après avoir pénétré dans le réseau interne. La cible est généralement la même que pour le test d'intrusion externe, mais la principale différence est que "l'attaquant" soit a une sorte d'accès autorisé, soit part d'un point du réseau interne. Plus précisément, dans le cas de Synack, le test des actifs internes (IAT) crée un canal privé entre les chercheurs de confiance et les actifs des clients, tels que les applications sensibles ou pré-livrées, derrière un pare-feu. En utilisant un VPN site à site, les avantages de LaunchPoint de Synack sont étendus de l'actif du client au chercheur.

**Liste de contrôle des missions** —Il s'agit d'un outil unique à Synack qui permet de déléguer au groupe de chercheurs des vulnérabilités suspectes à exploiter. La direction vient du système de balayage basé sur le ML (SmartScan). Le contrôle et le calendrier des exploits sont contrôlés par le scanner (et en fin de compte par le client). Synack propose des tests de type liste de contrôle qui complètent la découverte libre de vulnérabilités. Le résultat est une version de haute qualité des tests d'intrusion basé sur la conformité, dont le succès dépend du testing spécifique réalisé et enregistré. Les chercheurs de l'équipe Red de Synack exécutent un ensemble de missions (ou tâches) spécifiques et documentent leurs conclusions pour être payés. Les chercheurs sont rémunérés en fonction de la qualité de leur travail et des détails de leur soumission.

Les listes de contrôle sont souvent conçues à partir de directives basées sur l'OWASP ou le PCI/OWASP.

**Open Vulnerability Discovery (OVD)** —Parfois appelé "découverte créative de vulnérabilité", il s'agit d'un processus par lequel des chercheurs tentent d'accéder à un réseau, hôte, appareil ou application.

**Test d'intrusion**—Une cyber-attaque simulée autorisée sur un système informatique pour évaluer sa sécurité, en utilisant traditionnellement un ou deux chercheurs embauchés par une société de conseil, qui agissent selon une liste de contrôle ou, dans certains cas, recherchent les vulnérabilités de manière créative.

**Test fait à un moment précis**—Cette méthode se distingue du test continu et résulte généralement d'un besoin immédiat d'effectuer un test pour répondre à un événement important, tel qu'un audit, une demande d'un client clé ou une acquisition. Le délai standard est de deux semaines.

**Synack Red Team (SRT)**—C'est un terme de Synack qui représente le réseau privé de chercheurs en sécurité hautement fiables, diversifiés et contrôlés. La SRT permet aux chercheurs les plus talentueux du monde entier de faire ce qu'ils aiment au sein de la plateforme de Synack et d'être payés pour cela.

**Purple Teams**—Les équipes violettes améliorent le partage d'informations entre les équipes rouges et bleues afin de maximiser leur efficacité respective et combinée.

**Scanner**—Un dispositif qui analyse les vulnérabilités et les failles de sécurité. Il est automatisé et évolutif, mais peut produire d'énormes quantités de données qui chargent trop l'équipe de sécurité si elles ne sont pas triées par le fournisseur.

**Test d'ingénierie sociale**—Le test d'intrusion de l'ingénierie sociale est la pratique qui consiste à tenter des escroqueries typiques d'ingénierie sociale sur les employés d'entreprise afin de déterminer le niveau de vulnérabilité de l'entreprise à ce type d'exploit. Cette pratique est généralement hors du champ d'application d'un test d'intrusion.

**Triage**—Processus de tri des vulnérabilités signalées par un chercheur ou une équipe opérationnelle afin d'identifier finalement si une vulnérabilité est exploitable.

**TTP**—Il s'agit des tactiques, techniques et procédures utilisées par les agents de menace (cybercriminels) pour orchestrer et gérer les attaques. Dans la même veine, il peut également s'agir des méthodes utilisées par les chercheurs "chapeau blanc" pour identifier les vulnérabilités lors des tests d'intrusion.

**VDP** —Le programme de divulgation des vulnérabilités est un processus par lequel les hackers sont autorisés à signaler des vulnérabilités détectées dans les actifs d'une entreprise et à soumettre ces vulnérabilités officiellement à cette entreprise. Le VDP peut être géré par l'entreprise ou par une tierce partie sans contrôle ni protection, et se caractérise par un niveau de bruit élevé et la possibilité pour les acteurs malveillants d'opérer discrètement.

**Évaluation de vulnérabilités (ou Évaluation intelligente de vulnérabilités)**—bien qu'elle puisse être utilisée de manière plus large et générique, dans la pratique, elle désigne souvent les scanners réseau.

**Découverte de vulnérabilités**—une méthodologie de test qui s'appuie sur la variété, créativité et expertise de l'équipe Red de Synack pour imiter les méthodes des attaquants. Conçue pour trouver des vulnérabilités exploitables et inconnues dans les surfaces d'attaque des clients, la découverte de vulnérabilités permet d'obténir des résultats que les tests basés sur des listes de contrôle manquent souvent. Une fois que la validité d'une vulnérabilité soumise est confirmée, le chercheur de la SRT est rémunéré selon le modèle Bug Bounty. La découverte de vulnérabilités permet aux entreprises de gérer les risques associés à des vulnérabilités inconnues.

**Modèle White Bo**—Contrairement aux tests en boîte noire, les testeurs d'intrusion ont un accès complet au code source, à la documentation sur l'architecture, etc.