VOLUME 3

MESURER LA VALEUR DE LA SÉCURITÉ DANS
UN CONTEXTE D'INCERTITUDE

2020 LE RAPPORT DE CONFIANCE

Synack

La Confiance est essentielle.

Fournir des tests d’intrusion intelligents à grande échelle, la plateforme Synack a recours aux hackers éthiques les plus talentueux du monde, et à l'intelligence artificielle, pour assurer une couverture continue à la demande et avec des résultats exploitables.

Nous sommes Synack, la plateforme de sécurité collaborative la plus fiable au monde.

Synack®

Table des matières

Préface	4
Partie 1: Évaluation comparative	6
Partie 2: Résultats clés en matière de confiance en 2020	9
Partie 3: Sécurité dans un contexte d'incertitude	13
Partie 4: Éléments de base des tests de sécurité	17
Partie 5: Conclusion	28
Partie 6: Méthodologie	30

LES DIRIGEANTS DEMANDENT:

"Comment puis-je accélérer la transformation numérique de mon entreprise et m'assurer que ces nouveaux systèmes sont sécurisés?" "Puis-je être sûr que mon entreprise intègre correctement la cybersécurité dans nos systèmes sans perdre en rapidité?" "Comment puis-je être sûr que les applications développées dans le cadre du déploiement rapide et continu Agile et DevOps sont sécurisées?" "Comment mes systèmes et applications sont-ils sécurisés par rapport à mes concurrents et à d'autres secteurs?" "Le conseil d'administration peut-il être sûr que la transformation numérique qu'il a autorisé à mettre en œuvre est sécurisée et que le nom de notre société ne fera pas la une des journaux?"

La sécurité des actifs numériques de votre entreprise est aussi importante que la santé de votre corps. Quatre-vingt-dix-huit pour cent des citoyens américains n'ont pas été infectés par le COVID-19; cependant, si vous faites partie des 2 % qui l'ont été, vous en souffrez. Quatre-vingt-dix-sept pour cent des citoyens américains qui ont été infectés par le COVID-19 se sont complètement rétablis; cependant, 3 % ne l'ont pas fait. La probabilité que votre entreprise subisse de graves dommages à la suite d'une cyberattaque est faible, mais si elle se produit, les répercussions peuvent être dévastatrices. Beaucoup d'entre nous ont toujours protégé la santé en se soumettant à des examens physiques annuels. Beaucoup d'entre nous ont trouvé lors de ces examens des problèmes que nous pouvions corriger avant qu'ils ne deviennent graves. Dans mon propre cas, les médecins ont découvert une artère coronaire bloquée à 90 % lors d'un test d'effort cardiaque. Heureusement, je suis maintenant un heureux propriétaire d'un "stent" et pas une victime de crise cardiaque.

En cette période de COVID-19, nous avons vu que les tests ont sauvé des centaines de milliers de vies.

AVEC PLUS DE 30 ANS DE PRATIQUE DE LA CYBERSÉCURITÉ, JE PEUX VOUS DIRE QUE LES TESTS D'INTRUSION ONT DÉTECTÉ DES VULNÉRABILITÉS, DONT LA REMÉDIATION A PERMIS DE SAUVER DES DIZAINES DE MILLIERS D'ENTREPRISES CONTRE LA VIOLATION DE DONNÉES, L'INTERRUPTION DE LEURS ACTIVITÉS, LA PERTE DE PROPRIÉTÉ INTELLECTUELLE, LES RECOURS COLLECTIFS, LE HARCÈLEMENT DANS LES MÉDIAS ETC.

POUR LA CYBER-SANTÉ DE VOS ACTIFS NUMÉRIQUES LE TEST D'INTRUSION EXERCE UN EXAMEN DE STRESS ULTIME.

Les analyses de vulnérabilité standard vous aideront à détecter certaines vulnérabilités communes de faible criticité, mais les tests d'intrusion intelligents peuvent trouver ces "artères bloquées à 90 %" capables à vous tuer. Le Rapport de Confiance de Synack 2020 indique clairement que les entreprises qui survivent au déferlement continu de cyberattaques sont celles qui testent fréquemment le plus grand nombre possible de leurs actifs numériques avec la profondeur et l'étendue appropriées à la criticité de cet actif.

J'ai toujours trouvé ironique que la même technologie numérique que nous utilisons pour faire fonctionner nos entreprises, réduire les coûts, augmenter les ventes et les profits, et stimuler l'emploi, augmente simultanément la surface d'attaque. Dans l'environnement actuel, nous mettons en œuvre la méthode Agile et le DevOps. De nouvelles versions de notre logiciel sont installées chaque semaine. En d'autres termes, les tests que nous avons effectué le mois dernier avaient une surface d'attaque différente, rendant le test et les corrections insuffisants. Comment puis-je être sûr que la version de ce mois-ci n'a pas introduit de nouvelles vulnérabilités?

Synack offre une plateforme de test d'intrusion intelligente, établie, éprouvée et innovante. Des milliers de grandes enreprises mondiales l'utilisent pour détecter les vulnérabilités dans leurs actifs numériques que d'autres n'arrivent pas à trouver. Cela leur a permis de remédier aux vulnérabilités et, dans certains cas, d'éliminer les risques. Derrière la plateforme, la méthodologie de contrôle des chercheurs de Synack réunit les experts en sécurité les plus qualifiés et compétents du monde entier.

L'approche révolutionnaire de Synack en matière de tests d'intrusion permet de tester les actifs numériques de façon évolutive et continue au fur et à mesure du déploiement de nouveaux codes. Sa plateforme combine ce qu'un scanner automatique peut trouver en toute confiance, trié et analysé par des chercheurs pour validation, ainsi que les compétences des experts en sécurité pour détecter des vulnérabilités plus critiques qui échappent aux scanners automatisés. Comme toutes les vulnérabilités trouvées sont entièrement triées, confirmées par des chercheurs et présentées en détail dans des rapports exploitables, le nombre de faux positifs est fortement réduit et les mesures correctives sont plus rapides et efficaces.

Cette approche présente des avantages considérables. Tout d'abord, elle permet de découvrir les vulnérabilités qui apparaissent au fil du temps, soit par des changements dans le système de production, soit par des erreurs de configuration accidentelles. Ensuite, la participation de nombreux chercheurs aux tests d'intrusion permet d'obtenir une vision beaucoup plus complète des vulnérabilités, comme celle d'un cardiologue, d'un hématologue et d'un neurologue qui déterminent la cause d'une maladie. Enfin, la plateforme de Synack offre une analyse pragmatique de la facilité ou de la difficulté pour un attaquant à accéder à vos systèmes critiques et du type de dommages qui pourraient se produire si cet attaquant réussit.

Synack appelle cette analyse quantifiable Attacker Resistance Score (ARS)™ . L'ARS aide les responsables à déterminer le niveau de sécurité de vos actifs par rapport à vos homologues et concurrents ainsi qu'à d'autres secteurs, afin de vous donner une perspective réelle du risque de sécurité. En d'autres termes, si l'ARS indique que vos actifs sont attaquables, même par un «script kiddy» en quelques minutes, alors vous voudrez investir beaucoup plus dans votre posture de sécurité. Si l'ARS indique que vous êtes plus proche de Fort Knox, alors vous pouvez être sûr que vos investissements et vos pratiques de sécurité actuels vous protègent.

LE RAPPORT DE CONFIANCE DE SYNACK 2020 EST UN DOCUMENT INDISPENSABLE POUR QUICONQUE S'EST DÉJA FAIT DEMANDÉ PAR SON DIRECTEUR, PDG OU CONSEIL D'ADMINISTRATION: "POUVONS-NOUS FAIRE CONFIANCE À NOS SYSTÈMES NUMÉRIQUES? ET COMMENT NOUS COMPARER AUX AUTRES ENTREPRISES?" VOICI DEUX DES DIX QUESTIONS LES PLUS FRÉQUEMMENT POSÉES PAR DES CENTAINES DE SOCIÉTÉS.

MICHAEL CODEN
CHEF DE FILE MONDIAL DANS LE SECTEUR DE CYBERSÉCURITÉ
BCG PLATINION, BOSTON CONSULTING GROUP

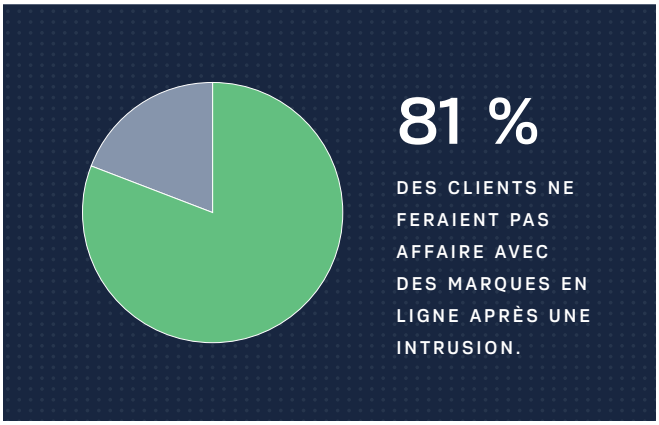
PARTIE 1

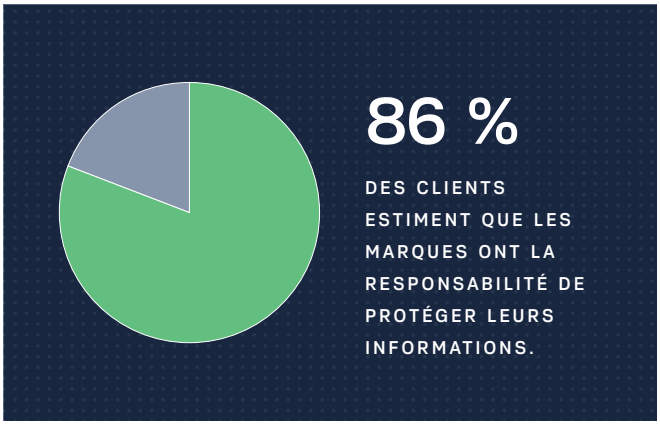
ÉVALUATION COMPARATIVE

Synack

La confiance n'a jamais été aussi importante.

En 2020, alors que nous sommes confrontés à des défis sans précédent pour nos communautés, les économies mondiales et l'environnement, les clients attendent de leurs marques préférées qu'elles soient des agents de changement positif, qu'elles apportent stabilité et sécurité dans l'incertitude et qu'elles développent des solutions innovantes pour construire des communautés plus saines et un avenir plus équitable.





SOIXANTE-DIX POUR CENT DES CLIENTS ESTIMENT QUE LA CONFIANCE DANS LES MARQUES EST PLUS IMPORTANTE QUE JAMAIS,
selon le Rapport spécial du baromètre de confiance d'Edelman : La confiance dans les marques en 2020. Cela conserne tout, des acquisitions importantes aux décisions d'achat quotidiennes. Lorsque les familles commandent une pizza via une application mobile, elles comptent sur leurs restaurants préférés pour qu'ils sauvegardent leurs données personnelles et financières tout en livrant une pizza fraîche et chaude à temps.

LA MÉFIANCE PEUT SE PROPAGER RAPIDEMENT.
L'un des moyens les plus rapides est une fuite de données. Quatre-vingt-un pour cent des clients ont déclaré qu'ils ne feraient pas affaire en ligne avec des marques après une intrusion. La Consumer Intelligence Series de PwC a révélé que 86 % des clients pensent que les marques ont la responsabilité de protéger leurs informations. La confiance des clients n'est pas la seule chose qui compte.

MALHEUREUSEMENT, LES INTRUSIONS SONT TROP FRÉQUENTS.
Le carnage qui en résulte peut nécessiter des réparations coûteuses et complexes. Le coût des intrusions massives de British Airways et de Marriott a dépassé les 100 millions de dollars. Les dirigeants qui gèrent mal les intrusions se font souvent licencier et peuvent être poursuivis au pénal. Au-delà des intrusions, les rapports sur les vulnérabilités importantes et dangereuses, même si elles ne sont pas exploitées, peuvent entraîner des risques de réputation et de revenus, une détérioration de la confiance, ainsi que des poursuites gouvernementales contre les entreprises technologiques mondiales.

Le Rapport de Confiance 2020 est le guide essentiel de Synack pour les RSSI, les DSI, les cadres dirigeants et autres responsables sécurité afin de comparer les mesures de sécurité dans les différents industries et secteurs de l'économie.

Le rapport s'appuie sur les données obtenues de la métrique brevetée **Attacker Resistance Score (ARS)™**[1] et tire ses informations directement de la plateforme de sécurité collaborative de Synack, basée sur des milliers de tests de sécurité effectués jusqu'en juillet 2020.

Les scores ARS vont de 0 à 100. Plus le score est élevé, plus une entreprise est capable de se défendre avec succès contre une cyberattaque.Quand il est plus bas, les entreprises sont plus exposées à des risques de sécurité.

En 2020, le score moyen de l'ensemble des industries était de 53, soit légèrement inférieur par rapport à la moyenne de 54 de l'année dernière, mais selon le Rapport de Confiance 2020 nous pouvons voir comment les scores peuvent changer d'une année à l'autre. Alors que certaines entreprises peuvent obtenir un ARS allant jusqu'à 100, un score supérieur à 70 est un indicateur d'excellentes pratiques de sécurité. Les clients de Synack accordent une grande importance aux tests de sécurité et analysent de manière proactive les nouveaux actifs et les applications numériques. Cela signifie que même si le score ARS baisse périodiquement, ces entreprises peuvent rapidement réagir à de nouveaux problèmes et sont donc mieux placées que les concurrents pour se défendre. L'objectif n'est pas d'obtenir le meilleur score et de passer à autre chose, mais de mesurer en permanence la résistance des nouveaux actifs et technologies aux attaques. Certaines entreprises peuvent obtenir un score supérieur ou inférieur à la moyenne du secteur, puisque les scores fluctuent, même pour les entreprises les plus proactives. fluctuate for even the most proactive organizations.

1 La métrique exclusive d'ARS (Attacker Resistance Score) de Synack est une mesure de résistance de vos actifs à une attaque. L'ARS global fournit une vue complète de la susceptibilité de l'actif cible à une attaque, basée sur un algorithme breveté développé par l'équipe scientifique de Synack. Il s'agit de la fonctionnalité de Coût de l'attaquant, de Gravité des résultats et d'Efficacité de remédiation. Des détails supplémentaires sur la métrique d'ARS sont disponibles en annexe.

LA MÉTRIQUE ATTACKER RESISTANCE SCORE™

Une métrique réaliste basée sur un modèle robuste

La métrique Attacker Resistance Score

=

Coût de l'attaquant

Le niveau d'effort effectué par l'équipe rouge de Synack pour couvrir la surface d'attaque et trouver les vulnérabilités

+

Gravité des résultats

La gravité et la quantité des vulnérabilités découvertes dans un actif

+

Efficacité de Remédiation

L'efficacité avec laquelle une entreprise résout les problèmes identifiés dans son environnement

PARTIE 2

RÉSULTATS CLÉS EN MATIÈRE DE CONFIANCE EN 2020

Synack

FIGURE 1: LE SCORE DE RÉSISTANCE AUX ATTAQUANTS EN 2020 PAR INDUSTRIE				
L'industrie[2]	2018 (Trust V1)	2019	2020[3]	Incidents/intrusions (le rapport Verizon DBIR)[4]
Gouvernement	57	47	61	6843/346[5]
Services financiers	61	57	59	1509/448
Santé	56	60	56	798/521
Technologie	53	46	55	5471/360[6]
SLED	49	46	50	819/228[7]
Conseil\Business et Services informatiques	50	53	48	7463/326[8]
Commerce en ligne	45	48	47	5471/360[9]
Commerce de détail	54	45	46	287/146
Industriels\Infrastructure critique	65	70	45	1070/407[10]
Moyenne	**56**	**54**	**53**	

Les agences gouvernementales renforcent les cyberdéfenses

L'année a été difficile pour de nombreux secteurs en raison des changements sans précédent nécessaires pour lutter contre la pandémie de COVID-19. Cela a surtout été le cas pour les agences gouvernementales et les ministères du monde entier. Mais ce secteur mondial a également montré que des tests continus et des mesures correctives rapides sont essentiels pour une cybersécurité efficace et exceptionnelle.

Les organismes gouvernementaux ont surpassé tous les autres secteurs évalués dans le Rapport de Confiance 2020 avec un score moyen de 61. Aux États-Unis, la nouvelle directive opérationnelle obligatoire 19-02 de l'Agence de cybersécurité et d'infrastructure sécurité, qui exige des organismes fédéraux qu'ils remédient aux vulnérabilités critiques dans un délai de 30 jours, a stimulé ces organismes à agir rapidement en cas de failles critiques. Cela a fait une différence essentielle. Dans l'ensemble, les organismes ont réduit de 73 % le temps nécessaire pour corriger les failles, ce qui a fait augmenter le score global du secteur.

En 2020, Synack a collaboré avec de nombreuses agences gouvernementales pendant la pandémie. La Synack Red Team, notre communauté des meilleurs chercheurs, assure la protection de ces agences qui utilisent de nouvelles technologies pour répondre à des besoins croissants et urgents. Un grand nombre de leurs actifs étaient essentiels pour la lutte contre la pandémie, ce qui aiderait notre nation à fournir des fonctions vitales.

2 Des descriptions plus détaillées des secteurs se trouvent en annexe
3 Janvier 2019- juillet 2020 (Nous avons étendu notre analyse dans le cadre du COVID)
4 Rapport de Verizon DBIR en 2020
5 Rapport de Verizon DBIR en 2020: Industrie publique
6 Rapport de Verizon DBIR en 2020: Informations
7 Rapport de Verizon DBIR en 2020: Services éducatifs
8 Rapport de Verizon DBIR en 2020: Services professionnels, scientifiques et techniques
9 Rapport de Verizon DBIR en 2020: Catégorie d'information utilisée
10 Rapport de Verizon DBIR en 2020: Fabrication, services publics

> *Notre test d'intrusion collaboratif a été la principale composante de notre réponse. Plus de 14 000 heures de tests, soit 350 jours complets par an".*

JANET VOGEL
RSSI
LE DÉPARTEMENT AMÉRICAIN DE LA SANTÉ ET DES SERVICES SOCIAUX

Les industriels et les infrastructures critiques en danger

D'autres secteurs ont connu une année plus difficile. L'ARS pour le secteur manufacturier et les infrastructures critiques est passé de 70 en 2019 à 45 en 2020. Cette baisse de 36 % est la plus importante de tous les secteurs dans le Rapport de Confiance 2020. Dans ce secteur, les entreprises ont obtenu un score allant jusqu'à 90 et beaucoup de ces entreprises en tête du classement ont recours aux tests continus. Le secteur manufacturier et les infrastructures critiques ont été soumis à une pression énorme en raison des changements rapides nécessaires pour se conformer aux directives visant à réduire la propagation du COVID-19. Cette pression se manifeste par un affaiblissement de leur posture de sécurité, alors qu'ils continuent à faire face à un flot constant d'attaques. Le rapport de Verizon en 2020, la Violation des données et les Investigations, a analysé 469 incidents graves affectant le secteur de fabrication, la plupart résultant d'attaques à motivation financière et d'attaques contre l'État-nation. Malheureusement, les industries critiques ne sont souvent pas bien protégées, car elles dépendent d'anciens systèmes. Selon une récente enquête menée par Greenbone Networks auprès d'entreprises d'infrastructures critiques, seuls 36 % ont déclaré avoir atteint un degré élevé de cyber-résistance.

La menace atteint le secteur de la santé au milieu du COVID-19

L'innovation dans le secteur de la santé a été essentielle pour la lutte contre la pandémie. Cette précipitation vers le développement et le déploiement de nouvelles applications entraînerait également des problèmes de cybersécurité. En outre, les forces de l'ordre du monde entier ont signalé une augmentation des tentatives de cyberattaques contre les hôpitaux. Malgré ces problèmes, le secteur a obtenu le troisième meilleur score moyen après les entreprises de recherche et de fabrication, restant vigilants et testant en permanence leurs actifs numériques. Alors que certains organismes ont augmenté leurs scores en donnant la priorité aux tests et aux mesures correctives pendant la pandémie, le score moyen du secteur de la santé est passé de 60 en 2019, à 56 en 2020, soit une baisse de quatre points. La SRT a testé de nombreuses technologies directement liées à ces efforts. Dans l'ensemble, les intrusions réelles dans les hôpitaux sont en baisse, ce qui indique que des tests de sécurité approfondis donnent des résultats.

Le commerce en ligne progresse alors que la demande numérique augmente

Le commerce de détail et le commerce en ligne ont subi des changements majeurs. Avec l'augmentation des achats en ligne et de la livraison à domicile, l'ARS moyen pour le commerce en ligne a bondi de deux points par rapport à 2018 et a augmenté de 7 % pendant le COVID, car les entreprises ont priorisé le testing des nouvelles applications et la remédiation rapide à des vulnérabilités. Dans le même temps, l'ARS du commerce de détail a diminué de 15 %, ce qui reflète une transition plus difficile vers le commerce entièrement numérique au cours des six derniers mois.

Les services financiers subissent des perturbations massives dues au COVID-19

En dépit de l'engagement opérationnel massif de déplacer les opérations des bureaux vers des services Zoom, les services financiers ont eu le deuxième meilleur ARS montant à 59 cette année, juste derrière le gouvernement.

Les services financiers se sont rapidement adaptés à la pandémie pour aider les employés à assumer leurs nouvelles réalités de travail à distance et pour garantir aux clients la possibilité de faire des affaires comme d'habitude, même si les banques et les sociétés de courtage ont fermé temporairement. Les tests de sécurité continus ont joué un rôle important dans l'augmentation de l'ARS dans le secteur. Les clients de Synack qui appliquent une approche des tests continus obtiennent un score de 18 % plus élevé que les autres entreprises.

La transformation numérique entraîne une baisse pour les services de conseil et les services informatiques

L'ARS a chuté pour les services de conseil et les services informatiques à 48 en 2020. Dans le cas de ce secteur, il semble que la transformation numérique continue à créer des difficultés. Les entreprises testent plus d'actifs et déploient plus de technologies, ce qui entraîne une augmentation de vulnérabilités détectées. Cela peut affecter le score total.

Mais le chemin vers la confiance n'est pas linéaire. Il faut faire des essais et des erreurs et se corriger rapidement pour que le changement s'opère. De nombreuses entreprises de cette catégorie ont réussi leur transformation numérique et continuent de voir leurs scores augmenter, certains atteignant même 96 sur 100. Les leaders de ce secteur obtiennent un score supérieur à la moyenne, ce qui constitue un exemple de test de sécurité proactif pour les autres acteurs de leur secteur. Par exemple, les consultants du gouvernement ont travaillé dur pour sécuriser notre chaîne d'approvisionnement nationale et tester ces actifs de manière proactive.

PARTIE 3

SÉCURITÉ DANS UN CONTEXTE D'INCERTITUDE

Synack

La pandémie mondiale a mis une pression énorme sur les RSSI et les autres professionnels en sécurité. Alors que les clients se précipitaient pour installer des plates-formes de télé-travail et des applications de vidéoconférence, ils s'attendaient — et exigeaient — que les entreprises protègent leur sécurité et leur vie privée. Les marques qui ne pouvaient pas maintenir cette confiance ont dû faire face à des conséquences réelles et mesurables.

Zoom en est un bon exemple. Il a connu une forte hausse d'utilisation ce printemps, les écoles et les entreprises étant toutes passées au travail à distance. Mais sa crédibilité a souffert des gros titres du Wall Street Journal et du New York Times, qui ont fait état de vulnérabilités majeures et du risque d'exploitation de la plateforme par des pirates informatiques. Le "Zoom bombing" est devenu un véritable problème pour les écoles et les universités. Le cours de ses actions s'est alors effondré. Des entreprises telles que SpaceX, Google et l'armée américaine ont interdit son utilisation et Zoom a fait l'objet de poursuites pour des problèmes de sécurité et de confidentialité. Le slogan "Zoom back-lash" est devenu une phrase accrocheuse courante.

Les dirigeants de Zoom ont réagi par une campagne de relations publiques vigoureuse et ont fait appel à des consultant en sécurité bien connus. Le PDG a effectué une grande tournée d'excuses. Il a même acheté une société de cybersécurité. La valorisation de Zoom est remontée à 100 milliards de dollars en août, mais les vulnérabilités imprévues et d'autres risques de sécurité ont ouvert la porte à une série de concurrents agressifs à un moment critique où les entreprises clientes doivent maintenir la confiance avec leurs clients.

Mais les entreprises préfèrent éviter d'être prises au dépourvu par des vulnérabilités majeures qui peuvent leur coûter une confiance inestimable sur le marché. Les tests continus sont un remède à ce genre de surprises désagréables - et dommageables.

Les changements de l'ARS lors du confinement

Peu de temps après l'entrée en vigueur des premières ordonnances de confinement aux États-Unis, les scores ARS ont chuté pour certaines industries clés telles que le commerce de détail, la fabrication et les infrastructures critiques. De plus, les exigences de quarantaine ont conduit la Red Team Synack à passé plus de temps à rechercher les vulnérabilités des clients. Le temps consacré par la SRT à l'analyse des actifs entre mars et avril 2020 a augmenté de 70 % par rapport à la même période l'année dernière.

> *"Une leçon positive de la pandémie COVID-19 est qu'il est devenu évident que la sécurité est un facteur de réussite pour l'entreprise.*

GREG MCCORD
CHEF DE FILE MONDIAL DE LA SÉCURITÉ D'INFORMATION
CalAmp

FIGURE 2: LES CHANGEMENTS DE LA MÉTRIQUE ARS PENDANT LE COVID-19

Industrie	Changement de l'ARS pendant le COVID-19†
Conseil\Business et Services informatiques	-3,88 %
Commerce en ligne	6,72 %
Services financiers	-11,64 %
Gouvernement	13,46 %
Santé	-0,74 %
Secteur manufacturier\ Infrastructure critique	-6,59 %
Commerce de détail	-7,15 %
SLED	26,16 %
Technologie	6,38 %

† Données propriétaires de Synack du 1er mars 2020 jusqu'au 1er juillet 2020

> *La confiance est absolument essentielle. Cela signifie que nous donnons la priorité à la sécurité de nos produits pour garder la confiance de nos clients. En tant qu'actuel PDG et ancien RSSI, je m'appuie sur des tests d'intrusion collaboratifs pour obtenir une vision réaliste de ma surface d'attaque sous l'angle de l'attaquant. C'est dans ce but que j'ai choisi Synack. Le portail SaaS de Synack rend mes résultats exploitables facilement accessibles. Ils me facilitent la vie en me permettant d'effectuer le triage et la vérification des patchs, et ils me permettent également de cocher les cases de conformité que vous savez que je dois vérifier.*

MICHAEL COATES
CO-FONDATEUR ET DIRECTEUR GÉNÉRAL, ALTITUDE NETWORKS
ANCIEN RSSI, TWITTER

Il est temps de doubler la sécurité

Pendant la pandémie, les RSSI se sont efforcés de veiller à ce que les principales opérations commerciales ne soient pas interrompues par des attaques. En fait, 70 % des entreprises interrogées ce printemps ont déclaré qu'elles prévoyaient de consacrer plus d'argent à la cybersécurité. Dans le même temps, les chefs d'entreprise se tournent davantage vers le cloud comme élément essentiel de leurs opérations. Le Boston Consulting Group a découvert que 45 % des entreprises interrogées s'attendaient à ce que la migration des applications vers le cloud soit une priorité majeure au cours des deux prochaines années.

C'est une préoccupation majeure en matière de sécurité. Une enquête menée en 2020 par IBM Security et le Ponemon Institute a révélé que 19 % des entreprises ne font pas de scan pendant la migration vers le cloud. Plus troublant encore, 57 % des personnes interrogées ont admis que leur entreprise ne savait pas quelles vulnérabilités représentaient les plus grands dangers.

PARTIE 4

ÉLÉMENTS DE BASE DES TESTS DE SÉCURITÉ

Synack

Les tests de sécurité ont un objectif simple : trouver des vulnérabilités potentiellement dévastatrices, les corriger rapidement et tirer les leçons du processus pour écrire un meilleur code.

Mais le processus est complexe. Il exige de la diligence et de l'expertise. Il faut les meilleurs chercheurs pour le faire correctement et des tests continus à partir de technologies intelligentes, basées sur l'IA. Il faut de l'attention et de la rigueur pour faire une réelle différence.

Les entreprises qui appliquent une approche des tests de sécurité continus ont un ARS en moyenne 18 % plus élevé que celles qui utilisent des tests faits à un moment précis.

FIGURE 3 : LA MÉTRIQUE ARS POUR LES TESTS CONTINUS PAR RAPPORT AUX TESTS FAITS À UN MOMENT PRÉCIS†

† Données propriétaires de Synack

Les tests continus ont permis d'augmenter l'ARS jusqu'à 23 pour cent

Les entreprises ne doivent pas être prises au dépourvu. Il existe une bonne solution pour cela.

Les entreprises qui adoptent les tests en continu en matière de tests voient leur ARS augmenter de 18 % en moyenne, certaines affichant jusqu'à 23 % de plus que celles qui n'effectuent que des tests périodiques. Les organisations qui testent leurs actifs régulièrement pendant trois ans ont enregistré une baisse de:

33,3 %
DES VULNÉRABILITÉS PAR INJECTION SQL

30 %
DES VULNÉRABILITÉS D'EXÉCUTION À DISTANCE

57 %
DES VULNÉRABILITÉS XSS

> *« En déplaçant la sécurité à gauche dans notre processus DevOps, nous commençons à découvrir des vulnérabilités que nous n'avions pas vues auparavant et nous découvrons de nouvelles vulnérabilités plus rapidement. Pour soutenir ce changement, nous avons dû construire un écosystème autour de la sécurité afin que les équipes de développement puissent ensuite y remédier au plus vite.*

RONALD ULKO
DOMINO'S
RSSI

Types de tests

SCANNER
L'utilisation de logiciels et d'intelligence artificielle pour rechercher des systèmes et des services vulnérables ou non autorisés.

TEST D'INTRUSION
L'évaluation des systèmes pour les vulnérabilités communes en s'appuyant sur l'Open Web Application Security Project (OWASP) ou un autre organisme de normalisation.

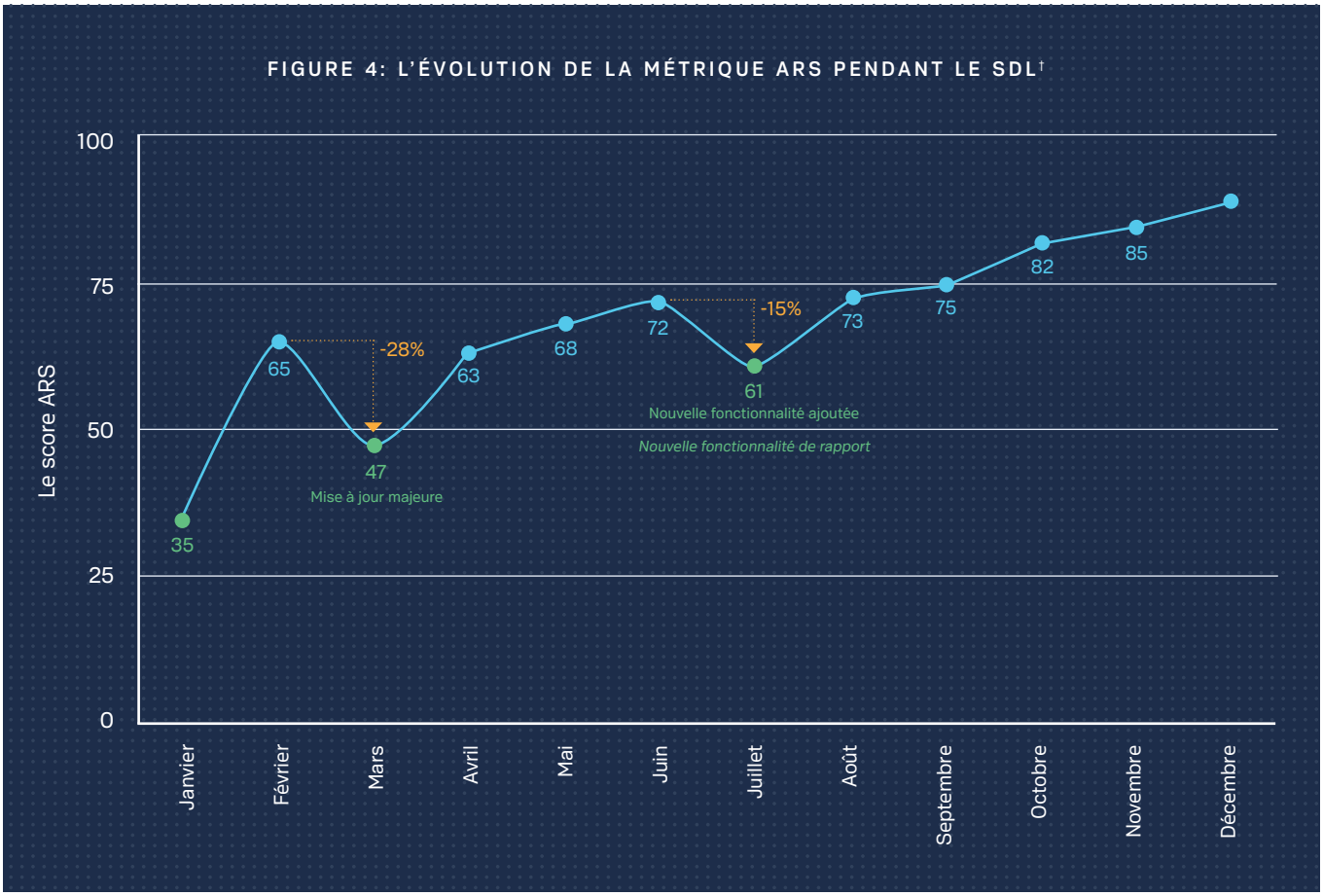
TESTS DE MODÈLE BUG BOUNTY
Les chercheurs sont autorisés à s'attaquer à l'actif selon leur méthodologie et leur créativité, encouragés par des primes.

PLATEFORME SÉCURITÉ DE TESTS COLLABORATIFS
Un processus qui combine les meilleurs éléments des trois autres catégories: c'est la prochaine génération de tests d'intrusion.

LE CHEMIN VERS LA CONFIANCE N'EST PAS LINÉAIRE.

L'augmentation du nombre d'équipes agiles et de la fréquence des mises à jour du code signifie que les tests ponctuels ne seront pas à la hauteur. Les actifs avec des mises à jour fréquentes et des données sensibles doivent être testés en permanence. C'est la seule façon d'obtenir une vue globale de l'environnement d'une entreprise en temps réel. Cela signifie que les actifs peuvent être évalués au moment de leur déploiement et que les vulnérabilités peuvent être découvertes et corrigées avant que les attaquants ne puissent les exploiter.

FIGURE 4: L'ÉVOLUTION DE LA MÉTRIQUE ARS PENDANT LE SDL†



† Données propriétaires de Synack basées sur de nombreux cas client

L'augmentation du coût des attaques

POURQUOI C'EST IMPORTANT

FIGURE 5: LE TEMPS MOYEN POUR TROUVER UNE VULNÉRABILITÉ†	
Industrie	Temps moyen de détection (heures)
Santé	15,5
Commerce de détail	16,0
SLED	16,7
Commerce en ligne	18,3
Services financiers	19,0
Conseil\Business et Services informatiques	19,8
Manufacturier\ Infrastructure critique	21,4
Technologie	29,2
Gouvernement	30,1
Total général	**21,0**

† Données propriétaires de Synack

Les entreprises les plus sécurisées - celles qui ont obtenu les meilleures scores dans le Rapport de Confiance - rendent les attaques contre elles longues et coûteuses. Cela signifie que les attaquants chercheront des cibles plus faciles. Les escrocs numériques ne veulent généralement pas dépenser de temps, d'énergie et d'argent pour accéder à leurs cibles. Pour renforcer la résistance aux attaques, une entreprise doit augmenter le coût de ces attaques.

Le coût de l'attaque est une composante du modèle ARS dans lequel nous mesurons et quantifions l'effort requis pour trouver une vulnérabilité. Le temps moyen nécessaire pour détecter une vulnérabilité a légèrement diminué, passant de 22,8 heures dans le rapport de l'année dernière à 21 heures. Les entreprises testent une plus grande variété d'actifs et certains d'eux contiennent des informations plus sensibles. Les chercheurs sont efficaces et des outils perfectionnés les aident à trouver les vulnérabilités de manière plus performante. Dans l'ensemble, les attaques sont de moins en moins coûteuses. Et c'est un problème. Une étude récente a montré que les attaquants peuvent effectuer une cyberattaque pour seulement 34 dollars par mois. Certaines cyber-opérations criminelles ne coûtent que 3 800 dollars par mois mais peuvent générer jusqu'à 1 million de dollars de bénéfices durant la même période.

Le secteur technologique est l'un des secteurs où le score mesurant le temps de détection des vulnérabilités est le plus élevé par rapport à d'autres industries. Comme de nombreuses entreprises technologiques ont adopté le développement agile et se sont concentrées sur la sécurité plus tôt dans le processus, leurs actifs sont protégés grâce à des tests réguliers. Cela signifie que les développeurs ont laissé moins de vulnérabilités dans le code. Cela signifie également que la découverte des vulnérabilités les plus graves a pris plus de temps.

FIGURE 6 : LA MOYENNE DU CVSS POUR LA PÉRIODE 2018-2020

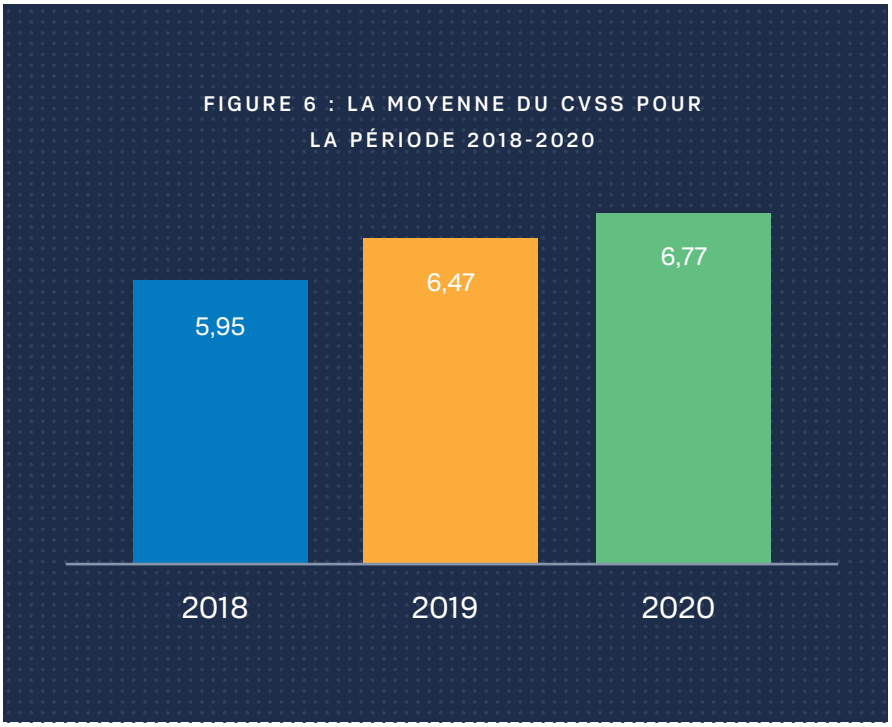


FIGURE 7 : LA MOYENNE DU CVSS PAR INDUSTRIE

Industrie	Moyenne du CVSS
Commerce de détail	6,13
Commerce en ligne	6,13
Technologie	6,26
SLED	6,33
Services financiers	6,41
Conseil\Business et services informatiques	6,48
Santé	6,66
Gouvernement	6,92
Manufacturier\Infrastructure critique	6,96

Remarque : les figures 6 et 7 sont basées sur les données propriétaires de Synack de 2018 jusqu'en juillet 2020

Comprendre la gravité des résultats

L'évaluation de la criticité des vulnérabilités selon le système standardisé CVSS aide les entreprises et les RSSI à comprendre la gravité des failles et c'est un élément du calcul de l'ARS. Les scores CVSS fournissent des informations précieuses, mais ils ne sont qu'un élément d'évaluation du risque global. Même les vulnérabilités qui ne sont pas classées comme graves peuvent entraîner des failles dévastatrices. Les hackers sont capables de compromettre les entreprises même avec des attaques basiques.

La criticité des vulnérabilités

LA MOYENNE DU CVSS A MONTÉ, MAIS LA CRITICITÉ EST RESTÉE ASSEZ CONSTANTE.

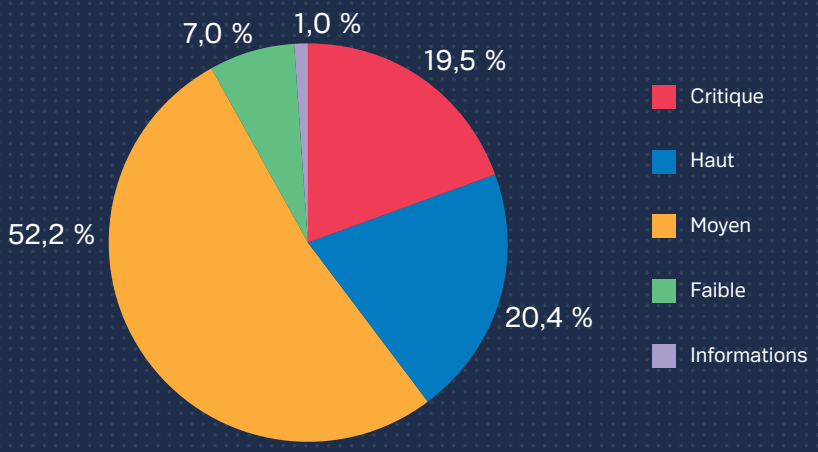
Les entreprises testent de plus en plus d'actifs divers, y compris leurs infrastructures. La moyenne du CVSS pour les actifs hôtes est 7,75 ce qui fait plus que celui du web et du mobile.

FIGURE 8: TYPE D'ACTIF MOYENNE DU CVSS

Type d'actif	Moyenne du CVSS
Hôte	7,75
Mobile	5,68
Web	6,6

FIGURE 9 : LA RÉPARTITION DES VULNÉRABILITÉS PAR CRITICITÉ

La moyenne du CVSS a montée, mais la répartition par criticité est restée assez constante.



Remarque : les figures 8 et 9 sont basées sur les données propriétaires de Synack de 2018 jusqu'en juillet 2020

La Répartition des Vulnérabilités par Catégorie

DE 2018 À 2020, LA RÉPARTITION DES VULNÉRABILITÉS DÉTECTÉES PAR SYNACK AU COURS DE MILLIERS DE TESTS DE SÉCURITÉ:

FIGURE 10: LA RÉPARTITION DES VULNÉRABILITÉS PAR CATÉGORIE†

Type de vulnérabilité % du total	2018	2019
Authentification\Session	8 %	6 %
Autorisation\Permission	19 %	22 %
Force brute	2 %	2 %
Injection de contenu	5 %	3 %
Chiffrement	<1 %	<1 %
CSRF	7 %	4 %
DoS	<1 %	<1 %
Logique fonctionnelle	7 %	7 %
Divulgation d'informations	16 %	14 %
Protection transport insuffisante	<1 %	<1 %
Autres	<1 %	<1 %
Exécution à distance	2 %	4 %
Erreur de configuration du serveur ou de l'application	2 %	5 %
Injection SQL	5 %	8 %
XSS	26 %	23 %

† Basé sur des données propriétaires de Synack

Gagner la confiance exige de la rapidité

FIGURE 11:

Pourquoi le dépistage précoce est utile

LE COUT DE LA REMÉDIATION AUGMENTE, PLUS LES VULNÉRABILITÉS SONT DÉCOUVERTES TARDIVEMENT DANS LE SDLC

Source : Celerity/IBM System Science Institute+le Rapport sur la Violation de données- IBM Ponemon 2019

Les entreprises se situant dans le premier quartile de la métrique ARS remédient aux vulnérabilités en moyenne dans un délai de 30 jours. Il est tout aussi important de corriger les vulnérabilités que de les détecter. Leur détection et remédiation rapides réduisent les coûts de manière significative.

La remédiation est le troisième élément de la métrique ARS de Synack et reste essentielle à la réduction des risques. À mesure que le nombre de vulnérabilités augmente, il devient difficile pour les équipes de rester proactives et de remédier à toutes les vulnérabilités. Nous recommandons un processus en trois étapes pour éliminer plus efficacement les risques :

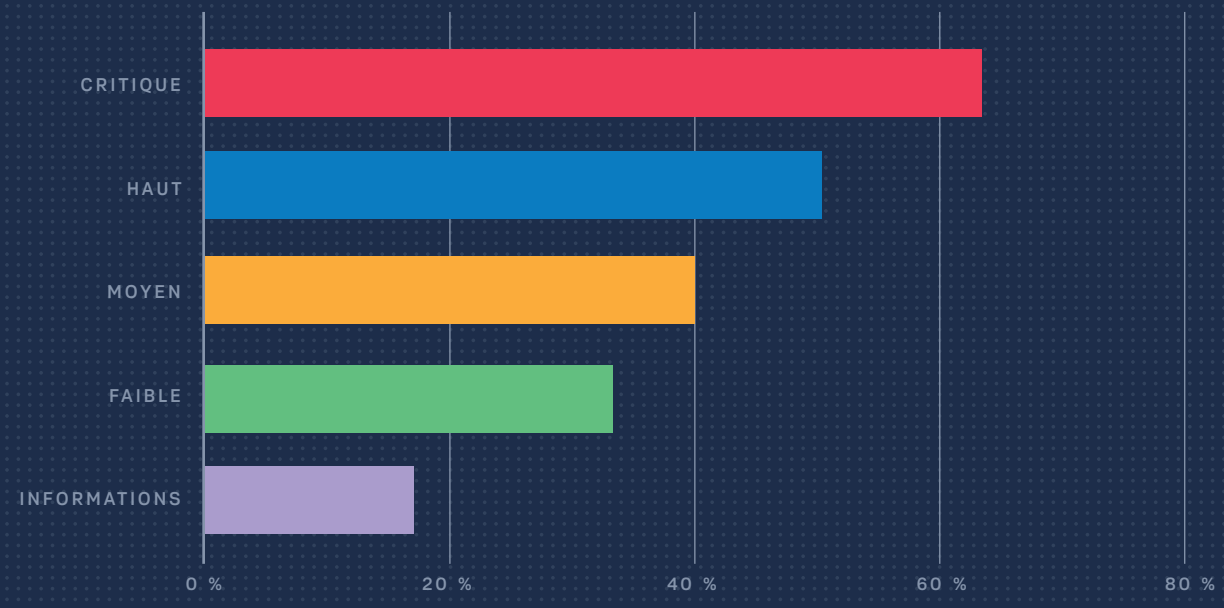
01 Prioriser les vulnérabilités les plus critiques.

02 Suivre un processus de remédiation simple et reproductible.

03 Apporter de la rapidité dans votre contexte sécuritaire — c'est un effet permanent.

Les vulnérabilités critiques corrigées en premier.

FIGURE 12: % DES VULNÉRABILITÉS DÉTECTÉES QUI ONT ÉTÉ CORRIGÉES



Source : Basé sur les données propriétaires de Synack jusqu'en juillet 2020

Il n'est pas surprenant que les vulnérabilités critiques soient prioritaires et corrigées plus rapidement que celles de gravité plus faible selon les propres données de Synack. Des milliers de nouvelles vulnérabilités sont révélées chaque année, et il est donc très important de savoir lesquelles doivent être corrigées ou atténuées immédiatement. Malheureusement, seuls 21 % des personnes interrogées dans l'étude de l'IBM Security et du Ponemon Institute sur la correction des vulnérabilités ont déclaré la correction efficace et rapide des failles au sein de leur entreprise. Dans certains cas, selon l'enquête, il faut parfois un mois pour remédier à une vulnérabilité critique ou à haut risque.

La priorisation des vulnérabilités peut aider les équipes à agir rapidement, mais en se concentrant uniquement sur les failles critiques, on ignore la possibilité que des attaquants enchaînent plusieurs vulnérabilités à faible risque. C'est une tactique courante et dangereusement efficace que les attaquants utilisent pour obtenir des privilèges d'administrateur — les "clés du royaume".

PARTIE 5

CONCLUSION

Synack

La confiance est fragile. Sa protection est cruciale.

Les clients ont besoin de faire confiance aux marques sur lesquelles ils comptent chaque jour. Ils doivent aussi la trouver dans leurs institutions. Sans confiance, les meilleures marques se battront sur le marché et les institutions ne pourront pas remplir des fonctions essentielles comme la prestation de services de santé ou même la tenue d'élections. La confiance est primordiale dans tous les aspects de la société, et se maintenir face à des menaces numériques de plus en plus graves est une tâche redoutable.

Il est également essentiel que les PDG fassent confiance à leurs systèmes et aux équipes chargées d'assurer la sécurité de leur entreprise. Comme nous l'avons vu cette année, les nouvelles sur des vulnérabilités dangereuses et des infractions massives peuvent causer d'immenses dommages financiers et ceux de réputation. Les piratages et les infractions peuvent également entraîner de lourdes amendes, des mesures gouvernementales et des poursuites judiciaires. Une approche proactive de la cybersécurité est plus vitale que jamais.

C'est la mission des RSSI. L'ARS offre la compréhension dont ils ont besoin pour assurer la sécurité des entreprises, éviter les infractions et les vulnérabilités coûteuses, protéger leurs clients et partenaires et maintenir une confiance et une fiabilité durables.

PART 6

MÉTHODOLOGIE

Synack

Sommaire de la méthodologie

Le métrique brevetee Attacker Resistance Score (ARS)™ de Synack est une mesure de la résistance de vos actifs à une attaque. L'ARS global fournit une vue complète de la susceptibilité de l'actif cible à une attaque, basée sur un algorithme breveté développé par l'équipe scientifique de Synack. Il évalue le coût de l'attaque, la gravité des résultats, les compétences de la SRT et l'efficacité des remédiatiions. L'ARS est calculé selon les données suivantes dans une combinaison pondérée:

COÛT DE L'ATTAQUANT

Cette variable répond à la question: "Combien d'efforts faut-il pour accéder à votre surface d'attaque et découvrir les vulnérabilités de vos actifs? " Le coût de l'attaquant est calculé en utilisant les données de capture de paquets collectées par LaunchPoint®, notre passerelle sécurisée. Les données brutes relatives au trafic détaillent toute l'activité de test que l'équipe Red de Synack a fait pour cette évaluation.

Pour calculer le coût de l'attaque, nous isolons d'abord les données de trafic de test d'intrusion afin de comprendre sa structure sous-jacente. Ensuite, à l'aide de ces informations structurelles, nous évaluons la "puissance" ou la durée du travail qui ont été nécessaires soit pour que le chercheur découvre avec succès la vulnérabilité, soit pour examiner pourquoi la vulnérabilité n'a pas été détectée. La quantité de "travail" de l'attaquant est estimée en comptant le nombre de "hits" (c'est-à-dire les requêtes HTTPS pour les applications web ou les paquets réseau envoyés pour les réseaux hôtes) par rapport au lieu d'évaluation. Le temps est mesuré à partir de la première connexion du chercheur à LaunchPoint et du "hit" sur le lieu d'évaluation jusqu'au moment où la vulnérabilité potentiellement découverte a été soumise ou qu'un laps de temps raisonnable s'est écoulé. De cette manière, un coût individuel de l'attaquant est calculé selon le fait que la vulnérabilité a été détectée ou pas. Ensuite, les scores sont normalisés sur une échelle de 0 à 100 en utilisant les valeurs brutes du coût de l'attaquant au sein de l'entreprise. Enfin, Synack détermine le coût de l'attaquant pour chaque actif en calculant la moyenne de ce coût et tous les efforts qui ont conduit ou pas à la détection des vulnérabilités. Compe tenu que l'absence de vulnérabilités découvertes indique la résistance au risque de cybersécurité.

LA GRAVITÉ DES RÉSULTATS

Dérivé de la gravité et de la quantité des vulnérabilités découvertes par rapport à vos actifs ciblés. Comme pour le coût de l'attaquant, la gravité des résultats est calculée pour chaque vulnérabilité. En particulier, l'importance de chaque vulnérabilité découverte est mesurée sur l'échelle du CVSS de 0 à 10, où 0 et 10 indiquent respectivement les vulnérabilités les moins et les plus graves. Selon le nombre et la gravité des vulnérabilités découvertes, un ensemble de modèles linéaires est utilisé pour générer un indicateur par vulnérabilité, qui est ensuite agrégée pour obtenir un indicateur par actif.

L'EFFICACITÉ DE LA REMÉDIATION

Mesure la rapidité et l'efficacité avec lesquelles une entreprise résout les problèmes identifiés dans son environnement. Après la découverte des failles dans l'actif du client, les données sur ces vulnérabilité sont envoyées au client pour l'atténuation et la remédiation. Après l'application du correctif, nous mesurons son efficacité et le temps qu'il a fallu pour qu'il soit appliqué. Nous prenons également en compte la quantité et la gravité des vulnérabilités pour lesquelles des correctifs ont été appliqués ou pas afin d'améliorer l'efficacité de la remédiation.

Définitions de l'industrie

CONSEIL/AFFAIRES ET SERVICES INFORMATIQUES
Les entreprises dont la principale source de revenus provient de la vente de prestations de services professionnels plutôt que des produits aux entreprises et aux agences gouvernementales.

ECOMMERCE
Les entreprises qui vendent la majorité de leurs produits via Internet.

ÉNERGIE/SERVICES PUBLICS
Les entreprises qui produisent et fournissent de l'énergie. Ce secteur comprend les entreprises impliquées dans l'exploration et le développement de réserves de pétrole ou de gaz, leur forage et raffinage, ainsi que les services publics distributeurs d'électricité, de gaz et d'eau.

DIVERTISSEMENT ET LOISIRS
Les sociétés qui se concentrent sur les produits et services liés aux loisirs, aux divertissements, aux sports et au tourisme, notamment les agences d'artistes et les sociétés d'édition musicale.

SERVICES FINANCIERS
Les sociétés qui gèrent l'argent des particuliers et des entreprises, notamment les caisses de crédit, les banques, les sociétés émettrices de cartes de crédit, les compagnies d'assurance, les sociétés de financement au consommateur.

SECTEUR FÉDÉRAL
Les organismes du gouvernement fédéral qui administrent, supervisent et gèrent les programmes publics tels que les branches des forces armées et d'autres départements exécutifs.

SOINS DE SANTÉ
Les entreprises qui fournissent des services médicaux aux patients et aux praticiens, qui fabriquent des équipements médicaux ou des médicaments, ou qui fournissent une assurance médicale.

SECTEUR MANUFACTURIER ET INFRASTRUCTURE CRITIQUE
La production de marchandises destinées à l'utilisation ou à la vente en utilisant la main-d'œuvre et les machines, outils, traitement chimique et biologique ou formulation. Leurs produits sont principalement vendus à d'autres fabricants ou à des détaillants. Ce secteur comprend également les sociétés d'énergie et de services publics.

COMMERCE DE DÉTAIL
Les entreprises qui vendent des produits ou des services aux clients par l'intermédiaire de divers canaux de distribution, mais qui se concentrent principalement sur la vente aux particuliers.

ÉTAT, AUTORITÉS LOCALES ET ÉDUCATION (SLED)
Ce marché représente cinq niveaux de gouvernement uniques : l'État, la ville, le comté, l'éducation et les districts spéciaux.

TECH
Les entreprises dont l'activité principale est la vente de technologies ou de services technologiques.