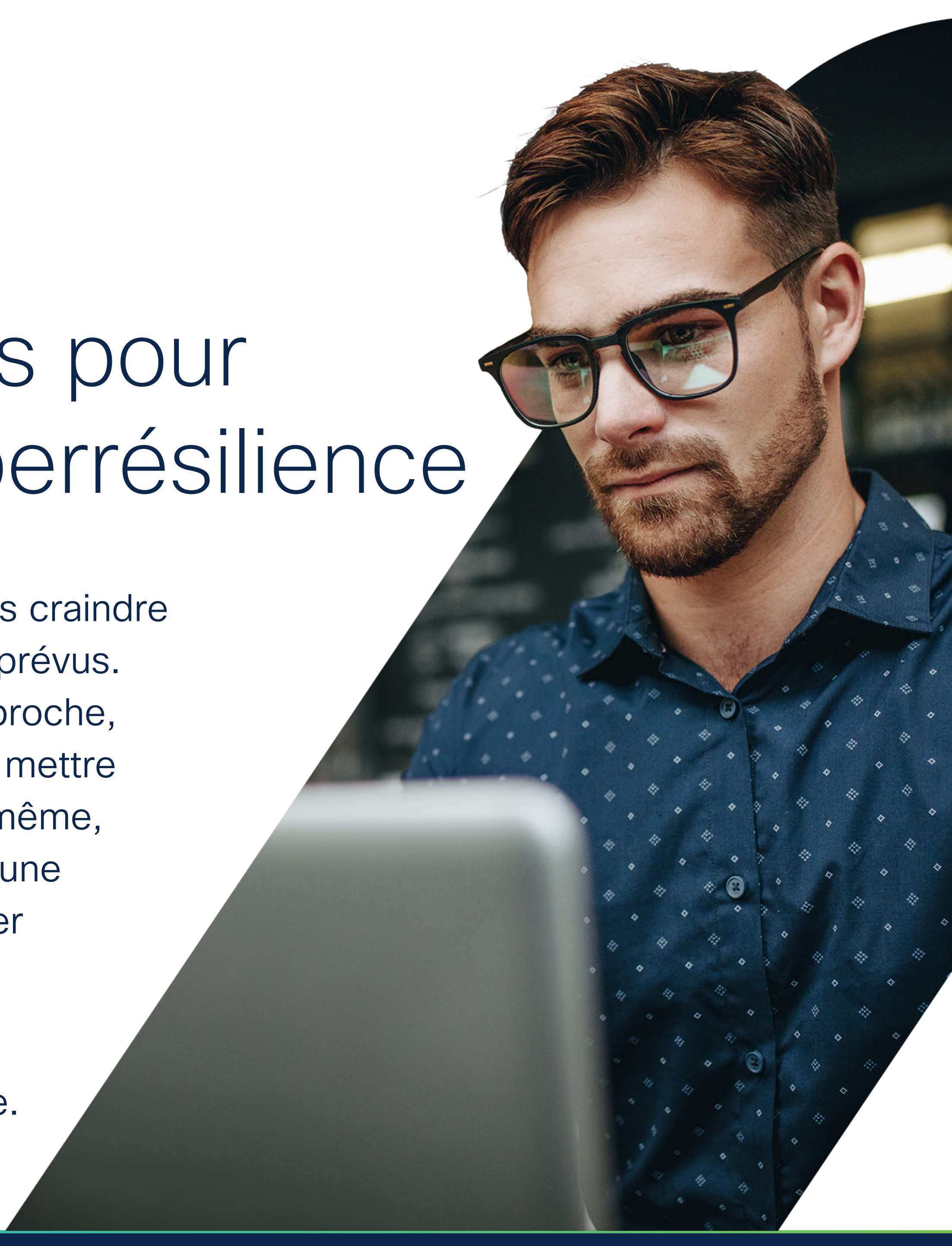
CISCO SECURE



5 étapes clés pour instaurer la cyberrésilience

La cyberrésilience consiste à ne pas craindre le changement et à anticiper les imprévus. Lorsque vous adoptez une telle approche, un simple clic accidentel ne saurait mettre en péril toute votre entreprise. De même, si vous devez soudainement ouvrir une succursale, vous pouvez la sécuriser dès sa mise en ligne.

Voyons dès maintenant les étapes clés pour bâtir votre cyberrésilience.

1

Promouvoir une culture de la sécurité

Dans une entreprise où la culture de la sécurité est forte, les collaborateurs sont traités comme une partie de la solution plutôt que comme le problème. Il est donc essentiel de prendre conscience du rôle qu'ils jouent. En effet, les collaborateurs participent à l'effort commun en signalant, par exemple, les tentatives de phishing, les programmes malveillants potentiels et d'autres incidents. À l'inverse, des violations fréquentes des politiques de sécurité et l'usage de solutions de contournement témoignent de profondes lacunes dans ce domaine.

46 % | Les entreprises qui encouragent une culture de la sécurité constatent une amélioration de 46 % de leur résilience.

Source : Rapport Cisco sur les objectifs en matière de sécurité, Volume 3

2

Renforcer l'implication des dirigeants

Les entreprises qui déplorent un faible soutien de la part de leurs dirigeants affichent un score de cyberrésilience inférieur de 39 % à celles qui bénéficient d'un soutien solide de la hiérarchie.

À elle seule, l'équipe de sécurité ne peut pas assumer l'entière responsabilité de la cyberrésilience. La direction doit être également impliquée.

Comment renforcer l'implication des dirigeants ?

- Comprendre les préoccupations de l'équipe dirigeante
- Expliquer en quoi votre plan de résilience contient des résultats axés sur l'entreprise
- Indiquer clairement les risques encourus en cas d'inaction
- Discuter des risques que vous êtes prêts à prendre ou non

3

Disposer des ressources nécessaires

Conserver du personnel et des ressources internes supplémentaires afin de mieux gérer les imprévus fait une grande différence.

Toutefois, si cela n'est pas possible pour vous, sachez que les entreprises qui s'attachent les services d'équipes de réponse aux incidents externes enregistrent une amélioration moyenne de 11 % de la cyberrésilience. Vous pouvez donc envisager de conclure un contrat avec un fournisseur fiable pour obtenir de l'aide rapidement.

15 % | Les structures qui disposent d'un pool de ressources flexible dans lequel elles peuvent puiser en cas de besoin atteignent en moyenne un score de cyberrésilience 15 % plus élevé que les autres.

Source : Rapport Cisco sur les objectifs en matière de sécurité, Volume 3

4

Exploiter la Threat Intelligence dans le cadre de votre stratégie de détection et de réponse

Les fonctionnalités de détection et de réponse fonctionnent mieux lorsqu'elles savent ce qu'il faut chercher et comment le trouver. Beaucoup d'entreprises utilisent à cette fin des solutions de Threat Intelligence de qualité.

Cela dit, il est impossible de tout protéger et d'anticiper avec exactitude la manière dont les menaces vont évoluer. Bien se préparer est essentiel. En veillant à ce que les systèmes ne présentent aucun point de défaillance unique, vous pouvez garantir la continuité de votre activité même si un composant doit être mis hors service en raison d'une menace.

Une solution cohérente de détection et de réponse étendues (XDR) repose sur deux piliers fondamentaux :

- Threat Intelligence
- Automatisation/Orchestration

Les entreprises disposant de telles fonctionnalités affichent un score de résilience global supérieur de 45 % par rapport à celui des structures qui n'ont mis en œuvre aucune solution XDR.

5

Opter pour des technologies flexibles et faciles à gérer

La bonne nouvelle est qu'il n'y a aucune différence en matière de cyberrésilience entre les environnements on-premise et cloud.

Toutefois, la simplicité et la fluidité sont des aspects cruciaux pour les deux types d'infrastructure.

À la fois simple à mettre en œuvre et à gérer, l'authentification multifacteur (MFA) constitue l'un des meilleurs moyens de renforcer votre résilience.

11 % | Le déploiement de la MFA peut augmenter votre score de cyberrésilience de 11 %.

Source : Rapport Cisco sur les objectifs en matière de sécurité, Volume 3

Lisez notre ebook pour en savoir plus :
Votre guide pour renforcer votre cyberrésilience avec Cisco Secure

Cisco Secure aide les entreprises du monde entier à se préparer aux imprévus. Non pas pour les éviter, mais pour y faire face, s'adapter rapidement et résister.

1043249609 | 03/23

CISCO The bridge to possible