Dossier de direction Cisco

JUILLET 2026

Un nouveau modèle opérationnel pour les infrastructures essentielles

Dossier de direction sur la cyberdéfense à l’ère de l’intelligence artificielle

Table des matières

LE PASSAGE À LA DÉFENSE CONTINUE 3

Deux forces qui redéfinissent le risque 3

Un nouveau rythme opérationnel 5

DE LA THÉORIE À LA PRATIQUE : SE DÉFENDRE À LA VITESSE DES MACHINES 6

Cisco met déjà ce modèle en pratique 7

DÉFINIR LE NOUVEAU MODÈLE OPÉRATIONNEL POUR LES INFRASTRUCTURE ESSENTIELLES 8

PAR OÙ COMMENCER : TROIS PRIORITÉS 9

1. Faire évoluer votre modèle opérationnel pour accroître la résilience de votre infrastructure 9

2. Moderniser votre infrastructure 9

3. Renforcer votre posture de sécurité 10

MESURER LES RÉSULTATS ET OBTENIR LE BUDGET NÉCESSAIRE 11

LES 90 PREMIERS JOURS 12

COMMENT CISCO PEUT VOUS AIDER 13

POURSUIVRE LA CONVERSATION 14

Le passage à la défense continue

Les modèles d'intelligence artificielle de pointe ont profondément transformé le cadre des menaces. Ces systèmes peuvent maintenant repérer des vulnérabilités, créer des codes d'exploitation et les enchaîner pour former des chemins d'attaque, le tout à la vitesse des machines. Il ne s'agit pas d'un cycle temporaire auquel quelques correctifs permettront de faire face. Il s'agit d'un changement permanent dans la vitesse à laquelle votre environnement peut être compromis.

Deux forces qui redéfinissent le risque

01 Le cycle d'application des correctifs ne suit plus le rythme

Le délai entre la divulgation d'une vulnérabilité et son exploitation active diminuait déjà rapidement. L'intelligence artificielle de pointe l'a maintenant ramené à quelques heures.

02 La barrière à l'entrée a disparu

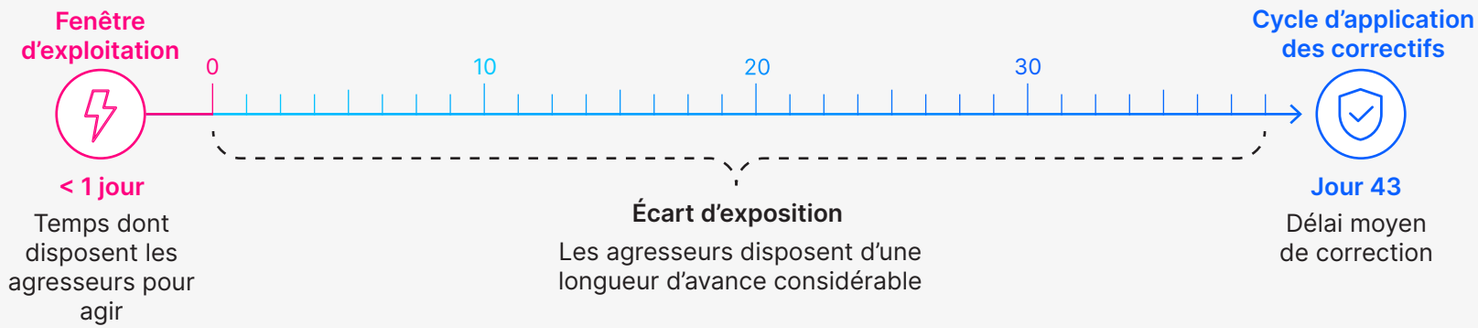
Grâce à l'intelligence artificielle, des agresseurs peu expérimentés peuvent désormais recourir à des techniques sophistiquées qui exigeaient autrefois les ressources d'un État.

Ces forces se renforcent mutuellement : l'accélération de l'exploitation multiplie les faiblesses à la portée d'un agresseur, tandis que l'abaissement de la barrière à l'entrée augmente le nombre d'agresseurs capables de les exploiter. Plus de possibilités d'attaque, entre les mains d'un plus grand nombre d'agresseurs, à une vitesse toujours plus élevée.

Les organisations peinent à se défendre contre cette nouvelle réalité pour deux raisons : des infrastructures vieillissantes qu'il n'est plus possible de corriger ou de mettre à niveau pour les protéger, et des processus dépassés qui traitent encore la sécurité de l'infrastructure comme une activité manuelle et périodique.

Le modèle traditionnel qui perdure (renforcer, valider et maintenir) repose sur l'idée que les adversaires respecteront les contraintes de votre calendrier de maintenance. Ce n'est pas le cas.

Les données montrent clairement les risques de cette approche : en 2025, 40 % des vulnérabilités les plus ciblées touchaient des systèmes en fin de vie. Le délai médian pour corriger une vulnérabilité critique demeure de 43 jours. Or, la fenêtre d'exploitation, c'est-à-dire la divulgation d'une vulnérabilité et sa transformation en arme, ne se compte désormais plus qu'en heures. Face à cette réalité, 43 jours ne représentent pas un simple retard. C'est là que tout se joue.



40 %

DES VULNÉRABILITÉS CIBLÉES TOUCHENT DES SYSTÈMES EN FIN DE VIE

Aucun correctif ne peut leur être appliqué. Ces systèmes demeurent exposés.

Pourquoi cet écart est-il si dangereux :

Vulnérabilité divulguée → Exploitation par les agresseurs en quelques heures → Correction en 43 jours → Les actifs en fin de vie demeurent exposés indéfiniment

Sources: *Talos Year in Review* et *2026 Verizon Data Breach Investigations Report*

Un nouveau rythme opérationnel

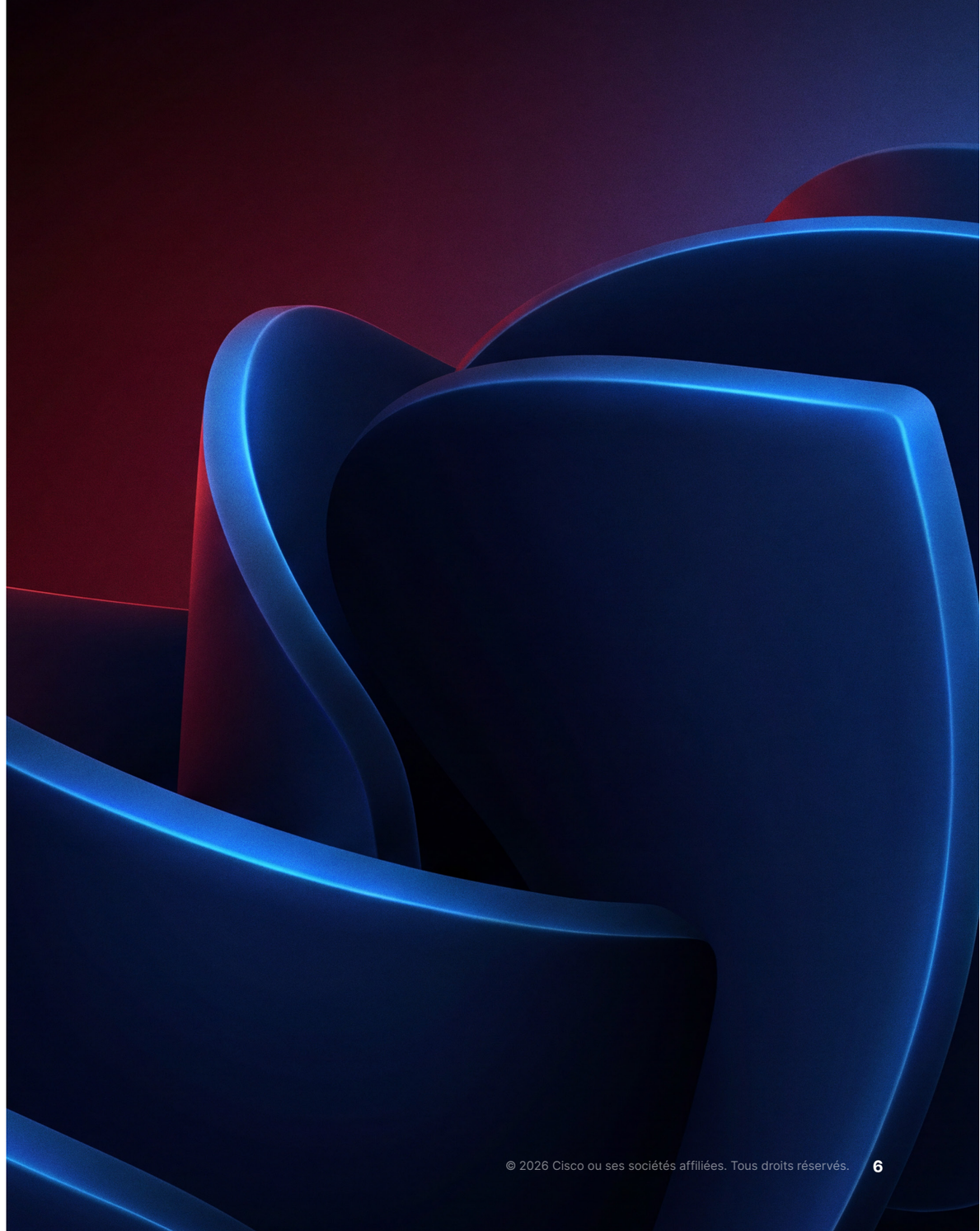
Les processus et les technologies d'hier ne permettent pas de devancer les menaces de l'ère de l'intelligence artificielle. Il faut adopter un rythme opérationnel continu : appliquer les correctifs et les mises à niveau selon une cadence fréquente et prévisible, retirer les actifs qui ne peuvent plus être sécurisés et réduire activement l'exposition tout au long de l'année.

Ce dossier de direction présente les mesures concrètes à prendre pour protéger votre organisation à l'ère de l'intelligence artificielle : faire évoluer votre modèle opérationnel, moderniser votre infrastructure et renforcer votre posture de sécurité. Examinez ces mesures conjointement avec vos responsables de la sécurité et de la mise en réseau. En vous concentrant sur un seul de ces domaines, vous exposeriez inutilement votre organisation à des risques.

Lorsque vous serez prêt à passer à l'action, votre équipe Cisco chargée du compte pourra vous présenter un guide détaillé qui offrira à vos équipes de mise en réseau et de sécurité des conseils pratiques plus approfondis sur les sujets abordés dans ce dossier.

De la théorie à la pratique : se défendre à l'échelle des machines

L'intelligence artificielle de pointe transforme l'attaque comme la défense, mais elle ne les place pas sur un pied d'égalité. Comme l'explique Rich Mogull, analyste en chef à la Cloud Security Alliance, dans un récent rapport, les agresseurs disposent d'un avantage mathématique : il leur suffit de trouver une seule vulnérabilité à exploiter. Les défenseurs, eux, doivent protéger chaque ressource contre tous les agresseurs, chaque fois. Les processus d'hier ne permettent pas de renverser ce rapport de force. Pour reprendre l'avantage, vous avez besoin d'un modèle opérationnel qui vous aide à renforcer le code, à appliquer les correctifs plus rapidement et à assurer une défense continue à grande échelle.



Cisco met déjà ce modèle en pratique

> « En seulement huit semaines, nous avons analysé 1,8 milliard de lignes de code dans l'ensemble de la gamme Cisco. Il aurait fallu huit ans à notre équipe de recherche en sécurité pour accomplir ce travail. Et ce n'est qu'un début. »
>
> **Anthony Grieco**
> Vice-président principal et chef de la sécurité et de la confiance Cisco

Pour se défendre, il ne suffit pas d'avoir accès à de puissants modèles d'intelligence artificielle. Il faut aussi disposer de l'expertise et du modèle opérationnel nécessaires pour transformer la vitesse et l'échelle de l'intelligence artificielle en résultats de sécurité reproductibles. L'organisation Cisco Security and Trust a d'abord validé cette approche dans le propre environnement de Cisco. Elle a combiné l'intelligence artificielle de pointe, une expertise en sécurité et des ressources spécialisées pour repérer et corriger les vulnérabilités plus rapidement, rendre les évaluations reproductibles et intervenir plus tôt en matière de prévention.

- **Repérer et corriger plus rapidement :** grâce à sa participation précoce au Project Glasswing d'Anthropic et au programme Trusted Access for Cyber (TAC) d'OpenAI, Cisco a appliqué des modèles d'intelligence artificielle de pointe à l'ensemble de sa gamme et analysé 1,8 milliard de lignes de code dans plus de 25 langages en huit semaines. Ces travaux ont montré comment les défenseurs peuvent tirer parti de la vitesse et de l'échelle de l'intelligence artificielle pour accélérer la détection et la correction des vulnérabilités dans des bases de code d'entreprise réelles.
- **Rendre les évaluations reproductibles :** s'appuyant sur ces travaux internes d'ingénierie de la sécurité, Cisco a publié en code source libre la Foundry Security Spec, un modèle éprouvé sur le terrain pour créer des systèmes agentiques d'évaluation de la sécurité. Cette spécification offre aux défenseurs une approche indépendante des modèles et des piles technologiques pour transformer des alertes parasites en observations circonscrites, hiérarchisées et vérifiables.
- **Intervenir plus tôt en matière de prévention :** Cisco a créé et publié en code source ouvert (Open Source) Project CodeGuard afin d'intégrer des règles de sécurité par défaut aux flux de travail de programmation fondés sur l'intelligence artificielle. Utilisées conjointement avec la Foundry Security Spec, les lacunes confirmées peuvent être converties en règles réutilisables qui contribuent à prévenir certaines catégories de bogues connus avant leur passage en production.

Définir le nouveau modèle opérationnel pour les infrastructures essentielles

Nous croyons que les organisations doivent adopter une défense continue qui repose sur trois dimensions : la cadence, la modernisation et la posture de sécurité.

Ce modèle continu transforme les façons de faire : l'application des correctifs devient une activité régulière plutôt qu'une intervention d'urgence, la modernisation élimine les risques au lieu de simplement renouveler le matériel, et une posture de sécurité dynamique limite les répercussions de toute intrusion.

	L'ancienne approche Renforcer, démontrer, puis ne plus modifier	**L'approche post-Mythos** Renforcer, démontrer et assurer une défense continue à la vitesse des machines
Cadence	Mises à niveau majeures tous les 12 à 24 mois	Préparation continue aux mises en production selon une approche CI/CD
Modernisation	Équipement, protocoles et scripts vieillissants maintenus en service	Retrait continu de tout cequi ne peut plus être sécurisé
Posture de sécurité	Exceptions de risque documentées	Réduction continue de l'exposition et confinement

Par où commencer : trois priorités

Le changement commence par trois priorités : exploiter une infrastructure résiliente qui soutient vos activités, remédier au vieillissement de l'infrastructure et renforcer votre posture de sécurité globale. Voici un aperçu de ces trois priorités et des questions à poser à votre équipe pour passer à l'action.

1. Faire évoluer votre modèle opérationnel pour accroître la résilience de l'infrastructure

L'application des correctifs n'est plus un projet périodique. Elle doit devenir une capacité permanente. Les chiffres imposent ce changement : le volume de correctifs augmente, les fenêtres de maintenance se raccourcissent et les processus manuels, appareil par appareil, ne suffisent plus à combler l'écart. Les adversaires, eux, peuvent exploiter ce délai. La solution consiste à adopter une cadence prévisible et automatisée. L'automatisation absorbe le volume afin que vos ingénieurs puissent se concentrer sur les décisions qui exigent leur jugement, plutôt que d'intervenir appareil par appareil. Cette cadence doit ensuite être rigoureusement appliquée : définissez des ententes de niveau de service pour la correction selon le niveau d'exposition, corrigez en quelques jours les expositions accessibles depuis Internet, puis traitez le niveau suivant à la prochaine fenêtre.

POSEZ LES QUESTIONS SUIVANTES À VOTRE ÉQUIPE :

- Quel est actuellement notre délai médian entre la publication d'un avis et la confirmation de la correction, selon le niveau d'exposition?
- Quelles étapes sont encore manuelles?

2. Moderniser votre infrastructure

Les actifs qui ne sont plus pris en charge présentent un risque qu'aucun contrôle ne peut compenser lorsqu'une nouvelle vulnérabilité apparaît, aucun correctif ne sera publié. Vous ne pouvez pas corriger un actif que le fournisseur ne maintient plus. Vous pouvez seulement le confiner ou le retirer. La modernisation ne se résume donc pas au renouvellement du matériel. Elle vise à éliminer les risques, et son analyse de rentabilité doit reposer sur l'exposition et les données du cycle de vie, plutôt que sur l'âge de l'équipement. Uniformisez votre environnement autour d'une architecture unique que vous pouvez corriger, surveiller, segmenter et valider. Financez-la ensuite comme une exigence de sécurité, par vagues successives, en commençant par les actifs les plus exposés.

POSEZ LES QUESTIONS SUIVANTES À VOTRE ÉQUIPE :

- Combien d'actifs ont dépassé leur date de fin de soutien ou s'en approchent?
- À quoi sont-ils connectés, et combien coûterait leur maintien en service pendant une année supplémentaire?

3. Renforcer votre posture de sécurité

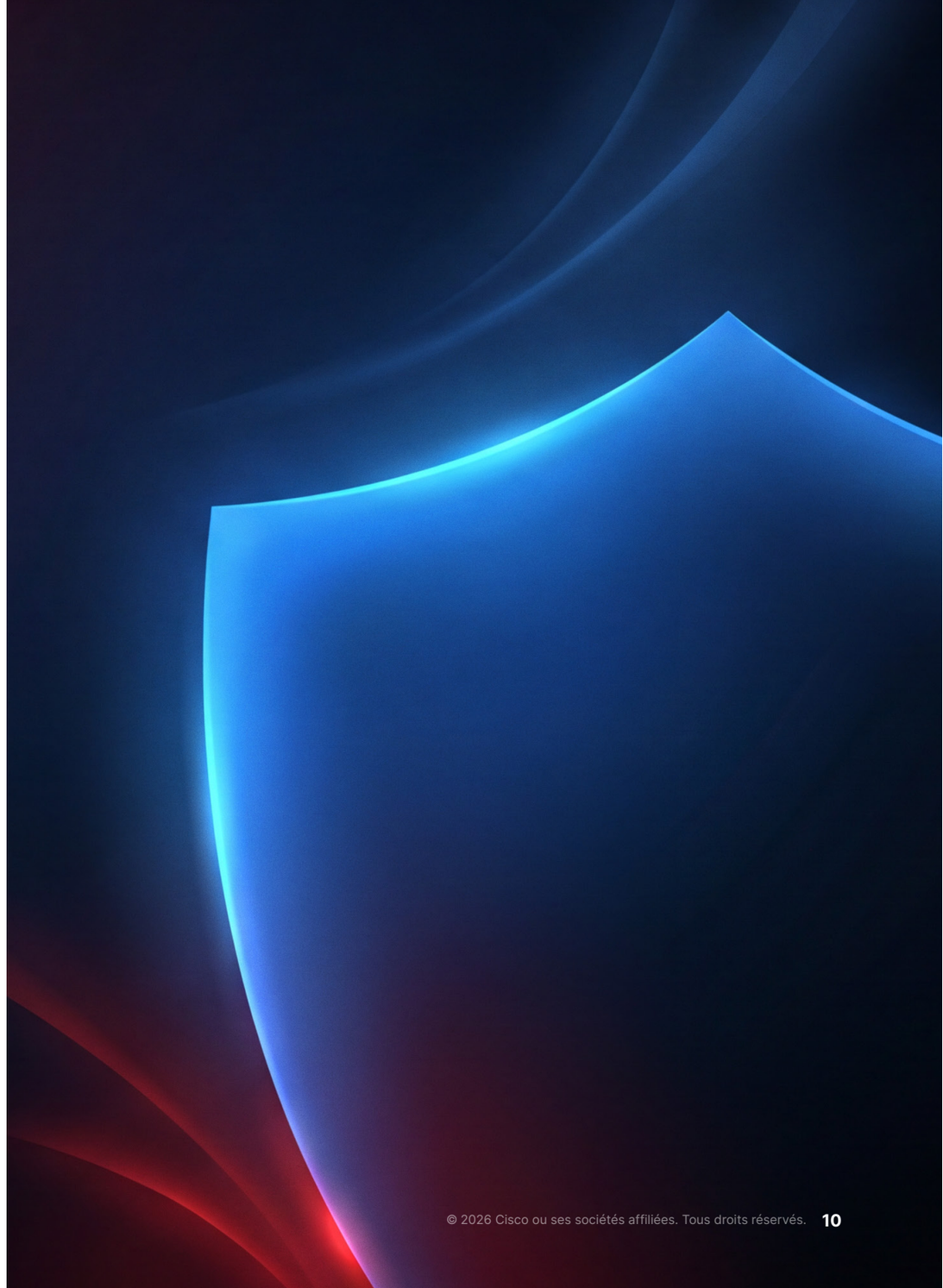
Les adversaires qui utilisent l'intelligence artificielle peuvent maintenant enchaîner les vulnérabilités à la vitesse des machines, ce qui met votre infrastructure en danger. Protégez les actifs exposés afin de réduire votre surface d'attaque. Segmentez votre environnement pour contenir les intrusions et en limiter les répercussions. Comblez les lacunes cachées liées aux identités afin de prévenir l'élévation des privilèges. Comme les attaques progressent désormais plus vite que les équipes humaines, votre centre des opérations de sécurité a besoin de la visibilité, de l'automatisation et des flux de travail d'intelligence artificielle agentique nécessaires pour suivre le rythme.

Ces contrôles ne sont pas tous nouveaux. Leur urgence, elle, l'est. En les mettant en place dès maintenant, vous garderez une longueur d'avance, non seulement sur les rares agresseurs avancés d'aujourd'hui, mais aussi sur ceux qui se généraliseront demain.

POSEZ LES QUESTIONS SUIVANTES À VOTRE ÉQUIPE :

- Si un agresseur parvenait aujourd'hui à prendre pied dans notre environnement, jusqu'où pourrait-il progresser dans le chemin d'attaque avant que nous réussissions à le contenir?
- Comment serions-nous au courant?
- À quelle vitesse pourrions-nous intervenir?

Une fois ces trois priorités établies, l'accent passe de la stratégie technique à l'exécution commerciale et à la mesure des résultats.



Mesurer les résultats et obtenir le budget nécessaire

Mesurez ce qui compte et présentez l'investissement sous l'angle du risque commercial afin d'obtenir le budget nécessaire.

Mesurer les résultats

- **Suivez le délai entre la publication d'un avis et la confirmation de la correction.** Mesurez-le selon le niveau d'exposition.
- **Mesurez le niveau de mise à jour de votre parc.** Suivez la proportion de votre environnement qui utilise la version la plus récente.
- **Faites respecter les contrats par niveau de service en matière de correction.** Privilégiez des contrats par niveau de service établis selon le niveau d'exposition plutôt que selon le nombre brut de vulnérabilités.
- **Conservez des preuves prêtes à être présentées au conseil d'administration.** Tenez les dossiers de conformité, les échéanciers de correction et l'état des actifs à la disposition des auditeurs et des cyberassureurs.
- **Établissez une responsabilité claire pour le travail agentique.** Veillez à ce que toute action importante puisse être vérifiée et annulée, et qu'elle relève d'un responsable clairement désigné.

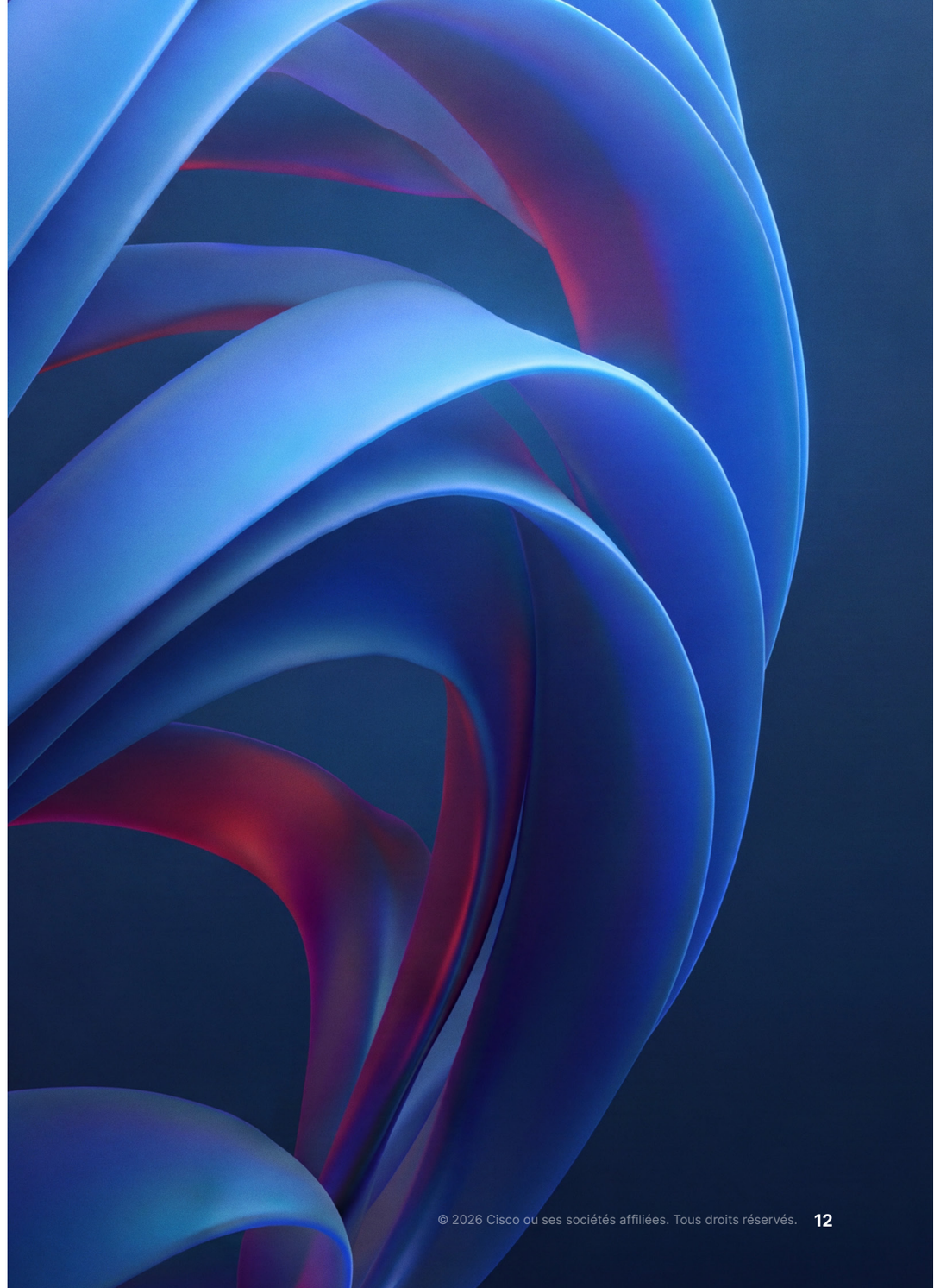
Financer le nouveau modèle

- **Échelonnez les dépenses.** Faites correspondre chaque vague de modernisation à un cycle budgétaire, en ciblant d'abord les actifs les plus exposés.
- **Alignez les dépenses sur l'échéancier.** Utilisez le financement pour convertir des dépenses en immobilisations imprévues en paiements prévisibles.
- **Présentez l'investissement comme une exigence de sécurité.** La menace dicte l'échéance. Il s'agit d'un impératif commercial, et non d'un simple souhait.
- **Financez la capacité opérationnelle.** Prévoyez un budget pour les services et les partenaires afin d'accroître la capacité d'action de votre équipe sans augmenter les effectifs.

Les 90 premiers jours

Voici cinq mesures que vous pouvez autoriser dès maintenant. Aucune n'exige que le programme complet soit défini au préalable, et chacune facilite la mise en œuvre de la suivante.

1. **Lancer une évaluation de l'exposition.** Établissez une vue à jour et hiérarchisée de vos actifs, des vulnérabilités, des éléments qui ne sont plus pris en charge et des risques auxquels vous êtes exposé. Elle deviendra votre source d'information commune et fiable.
2. **Définir des contrats par niveau de service pour la correction selon le niveau d'exposition.** Engagez-vous à corriger en quelques jours les expositions accessibles depuis Internet ou présentant un degré de criticité élevé, puis à traiter le niveau suivant à la prochaine fenêtre. Rendez ensuite compte des résultats obtenus. C'est cette décision stratégique qui concrétise la défense continue.
3. **Mettre en place la cadence.** Uniformisez les fenêtres de changement et préapprouvez les modèles afin que l'application des correctifs devienne une activité de maintenance courante plutôt qu'une exception.
4. **Déterminer les cibles de la première vague de modernisation.** Repérez les actifs non pris en charge les plus exposés et financez leur remplacement en priorité. Fondez l'analyse de rentabilité sur l'exposition, les données du cycle de vie et les besoins commerciaux futurs. La modernisation est l'occasion de mettre en place une infrastructure plus sécurisée et prête pour l'avenir.
5. **Organiser un exercice de simulation d'intervention à l'ère de l'intelligence artificielle.** Simulez un adversaire qui exploite une vulnérabilité à la périphérie pour se déplacer latéralement à la vitesse des machines, afin d'harmoniser l'intervention des équipes.



Comment Cisco peut vous aider

Cisco et ses partenaires de confiance sont là pour vous aider à composer avec cette nouvelle réalité. Avec ses partenaires, Cisco offre des services professionnels pour accompagner votre organisation dans tous ces domaines, notamment Cisco Resilient Infrastructure Services, qui propose une démarche structurée en trois phases pour renforcer l'infrastructure.

Faire évoluer votre modèle opérationnel pour accroître la résilience de l'infrastructure :

À compter de juillet 2026, Cisco publie ses versions selon un calendrier fixe annoncé à l'avance. Les périodes de publication sont échelonnées afin qu'aucune équipe n'ait à gérer deux fenêtres majeures simultanément. Nous associons chaque avis à vos actifs, le classons selon le niveau d'exposition plutôt qu'en fonction du seul score de gravité, puis confirmons que le correctif a bien été appliqué. Lorsqu'un correctif ou une mise à niveau ne peut pas encore être déployé, des protections à l'exécution sécurisent l'actif sans entraîner de temps d'arrêt.

Moderniser votre infrastructure :

Nous offrons plusieurs moyens de repérer les actifs Cisco qui ne sont plus pris en charge et qui demeurent exposés, ainsi que des recommandations pour renforcer l'infrastructure et activer des protections de sécurité supplémentaires. Lors du renouvellement de votre infrastructure, Cisco recommande d'adopter une architecture de réseau sécurisée qui intègre la sécurité au réseau même, grâce à une segmentation axée sur l'identité, à des politiques communes et à une application distribuée. Cisco Capital offre également des options de financement pour vous aider à gérer les dépenses imprévues.

Renforcer votre posture de sécurité :

Cisco sécurise l'ensemble du chemin d'attaque. La gouvernance des identités couvre les personnes, les machines et les agents d'intelligence artificielle, une distinction de plus en plus importante à mesure que ces agents se multiplient. La segmentation permet de contenir les déplacements latéraux en cas d'intrusion. Enfin, la détection et l'intervention sont accélérées à la vitesse des machines : l'intelligence artificielle absorbe le volume, tandis que vos analystes conservent la responsabilité des décisions qui exigent leur jugement.

Poursuivre la conversation

Lorsque vous serez prêt à passer à l'action, communiquez avec votre équipe Cisco chargée du compte pour transformer les recommandations de ce dossier en mesures concrètes. Elle pourra vous accompagner tout au long de ce parcours et vous présenter un plan ainsi qu'une évaluation plus détaillés, adaptés à votre organisation et à ses défis.

Vos partenaires Cisco constituent également une ressource précieuse. Leurs capacités varient. Choisissez donc un partenaire dont les forces correspondent aux besoins de votre environnement. Consultez le carrefour des partenaires Cisco pour trouver le partenaire qui vous convient.