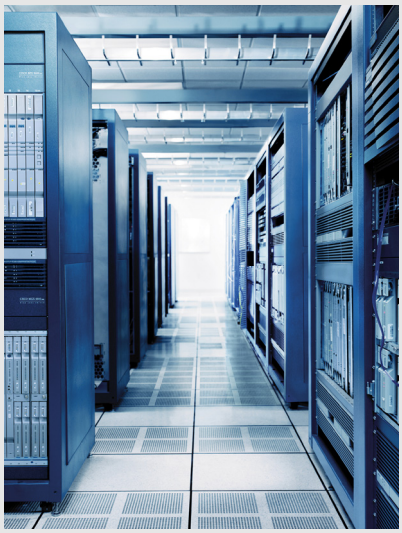
# Service d'évaluation de l'architecture de sécurité Cisco

Comprendre et renforcer l'architecture de sécurité de l'infrastructure de votre entreprise



**Une approche architecturale de la sécurité**

Bénéficiez d'une vue complète de votre infrastructure de sécurité :

- **Alignez les objectifs de sécurité avec ceux de l'entreprise :** identifiez et hiérarchisez les risques ainsi que les opportunités de correction.
- **Utilisez des méthodologies basées sur les normes :** utilisez le Cadre de contrôle de la sécurité de Cisco pour bénéficier d'une visibilité et d'un contrôle accrus.
- **Réduisez les risques liés au non-respect des réglementations :** améliorez la confidentialité, l'intégrité et la disponibilité des processus métier et informations de l'entreprise.
- **Personnalisez votre approche :** sélectionnez les évaluations qui répondent à vos besoins en matière de sécurité.

## Présentation

Dans le paysage complexe et en constante évolution des menaces actuelles, toute faille au niveau d'une solution de sécurité peut compromettre l'intégrité des données, la confidentialité des informations et la sécurité des applications stratégiques de l'entreprise. Votre infrastructure a besoin de contrôles de sécurité intégrés qui protègent votre infrastructure au sein d'un environnement de menaces et de vulnérabilités dynamique, tout en restant adaptée aux exigences en matière de politique de sécurité et de respect des normes d'une entreprise en pleine évolution.

Pour les experts en sécurité, il n'est plus question de chercher à résoudre les problèmes de sécurité d'une infrastructure par l'emploi de produits isolés. Ils considèrent désormais que ces problèmes nécessitent une solution complète intégrée à l'ensemble de l'infrastructure. Pour y parvenir, la meilleure solution consiste à adopter une approche architecturale systématique qui tient compte du cycle de vie informatique dans son intégralité et qui s'appuie sur un cadre de sécurité basé sur les normes. Les évaluations d'architecture de Cisco® sont réalisées à l'aide du Cadre de contrôle de la sécurité de Cisco. Ce cadre de contrôle, indépendant du fournisseur, est élaboré à partir de normes industrielles, de principes d'infrastructure de sécurité et de l'expérience en ingénierie de Cisco en matière de sécurisation des infrastructures d'entreprise.

Axé sur les contrôles technologiques qui étayent les objectifs de sécurité de base que sont la visibilité et le contrôle, le Cadre de contrôle de la sécurité de Cisco est utilisé pour évaluer l'architecture qui protège votre infrastructure réseau étendue, les périphériques connectés et les données de l'entreprise. Ce cadre est cohérent avec les normes de conformité industrielle et réglementaire de sécurité courantes, ainsi qu'avec les normes internationales, et notamment la série ISO (International Organization of Standardization) 27000 et la norme NIST (National Institute of Standards and Technologies) 800-53.

Le service Cisco Security Architecture Assessment Service (Service d'évaluation de l'architecture de sécurité) vous permet de mettre en œuvre une architecture de sécurité complète en identifiant les failles de votre architecture de sécurité et en fournissant un ensemble hiérarchisé de mesures pratiques pour les corriger. Les évaluations sont adaptées aux infrastructures Cisco et multifournisseurs pour le réseau de routage et de commutation central, pour les domaines fonctionnels principaux (et notamment les communications de centres de données et unifiées) et pour les points de terminaison connectés au réseau.

## Expertise appliquée

Les évaluations sont effectuées par des consultants Cisco qui mettent à profit leur vaste expérience en matière de sécurité dans différents secteurs verticaux et agences gouvernementales. Cette expertise est complétée par l'association d'outils de pointe, de méthodologies et d'un accès direct à des ingénieurs de développement de produits Cisco qui vous aident à tirer le meilleur parti des fonctions de sécurité sophistiquées intégrées à vos produits Cisco.

Les experts en sécurité de Cisco commencent par réaliser un examen détaillé de vos objectifs et besoins en matière de sécurité. À partir de ces informations, ils réalisent une analyse approfondie de votre infrastructure de sécurité, et notamment de la topologie du réseau, des périphériques réseau, des dispositifs de sécurité, des périphériques d'applications et des points de terminaison. Ils évaluent en outre l'évolutivité, les performances et la gérabilité de votre architecture de sécurité globale.

En se basant sur des données collectées avec soin, les ingénieurs Cisco peuvent identifier les vulnérabilités et les risques opérationnels de votre infrastructure en effectuant une analyse complète de son adéquation avec les meilleures pratiques du secteur. Les ingénieurs fournissent ensuite des recommandations hiérarchisées et pratiques pour limiter les risques opérationnels identifiés, et notamment des améliorations à apporter à la topologie, aux protocoles, aux stratégies, aux configurations de périphériques et aux outils de gestion. En adoptant cette approche exhaustive lors de l'évaluation de votre infrastructure de sécurité, ce service aide votre entreprise à améliorer la gestion des risques et à répondre aux besoins en matière de conformité, en réduisant les menaces qui pèsent sur la confidentialité, l'intégrité ainsi que la disponibilité des processus métier et informations de l'entreprise (voir tableau 1).

**Tableau 1.** Résumé de l'activité et des avantages du service Cisco Security Architecture Assessment Service (Service d'évaluation de l'architecture de sécurité)

| Résumé de l'activité | Résumé des avantages |
|---|---|
| • Examiner les objectifs et les besoins de l'entreprise en termes de sécurité.<br>• Examiner l'architecture de sécurité et la documentation de conception existantes, et notamment les conceptions physiques et logiques, les diagrammes de topologie du réseau, les configurations de périphériques et les plans détaillés, en fonction des besoins.<br>• Pour chaque domaine fonctionnel inclus dans la portée de l'engagement, évaluer si chacun des contrôles recommandés dans le Cadre de contrôle de la sécurité de Cisco est présent dans l'infrastructure de sécurité.<br>• Évaluer l'efficacité de chaque contrôle technique à fournir la fonction de sécurité désignée.<br>• Évaluer l'évolutivité, les performances et la gérabilité de l'architecture de sécurité.<br>• Identifier les vulnérabilités de l'infrastructure de sécurité.<br>• Fournir un rapport qui documente les failles au niveau des contrôles et fournit une analyse des risques de sécurité ainsi que des recommandations hiérarchisées et pratiques pour les corriger.<br>• Présenter les résultats et les recommandations hiérarchisées. | • Créer une architecture de sécurité robuste et évolutive en utilisant une approche axée sur l'entreprise et évitant les risques.<br>• Protéger de façon plus efficace votre infrastructure en identifiant les vulnérabilités architecturales et les écarts par rapport aux meilleures pratiques en matière de sécurité.<br>• Protéger la productivité des employés, les principaux éléments de propriété intellectuelle et les données sensibles du client en limitant les risques de sécurité.<br>• Répondre aux exigences en matière de respect des normes en identifiant des améliorations à apporter aux contrôles internes afin de mieux protéger les données.<br>• Renforcer la capacité de votre personnel à éviter les menaces futures, à les détecter et à y répondre.<br>• Protéger votre investissement en développant les fonctionnalités de sécurité de l'infrastructure existante. |

Pour une meilleure adaptabilité aux besoins uniques de votre entreprise en termes d'activité, d'infrastructure et de budget, le service Cisco Security Architecture Assessment Service (Service d'évaluation de l'architecture de sécurité) et le Cadre de contrôle de la sécurité de Cisco sous-jacent peuvent être personnalisés de façon à se concentrer sur différents domaines fonctionnels de votre infrastructure. L'évaluation interne de l'architecture de sécurité examine les contrôles internes portant sur l'infrastructure de sécurité commune et les domaines fonctionnels du réseau. Au-delà de l'évaluation interne, sept autres domaines fonctionnels peuvent être évalués de façon indépendante. La section suivante décrit chacun des domaines fonctionnels et les évaluations associées.

Le service Cisco Security Architecture Assessment Service (Service d'évaluation de l'architecture de sécurité) comprend une évaluation obligatoire et sept facultatives :

- Évaluation de l'architecture de sécurité interne (obligatoire)
- Évaluation de l'architecture de sécurité périmétrique
- Évaluation de l'architecture de sécurité des communications unifiées

- Évaluation de l'architecture de sécurité sans fil
- Évaluation de l'architecture de sécurité du centre de données
- Évaluation de l'architecture de sécurité des points de terminaison
- Évaluation des règles de pare-feu
- Évaluation de l'architecture de sécurité physique

**Évaluation de l'architecture de sécurité interne (obligatoire)**

Les attaques côté client multiprotocoles sophistiquées qui sont lancées en interne sont potentiellement plus gênantes et coûteuses que les brèches de sécurité externes. Ce service examine l'architecture de sécurité requise au niveau du réseau interne pour le protéger contre ces menaces, et notamment des réseaux WAN et LAN pour les sites centraux, de campus et individuels. Il couvre également les contrôles d'infrastructure de sécurité communs qui s'appliquent au contrôle d'accès, à la gestion des identités, à la gestion du réseau, à la détection des intrusions, à la gestion des événements de sécurité et à la journalisation. Cette évaluation est obligatoire car elle est utilisée comme base pour les autres évaluations.

**Évaluation de l'architecture de sécurité périmétrique**

La connexion de votre réseau interne à Internet, vos partenaires, vos clients et votre main-d'œuvre mobile sont les principaux accélérateurs d'activité, mais ils exposent votre infrastructure, votre propriété intellectuelle, les données de vos clients et la disponibilité de vos principaux services à des menaces importantes. Cette évaluation analyse l'architecture de sécurité qui protège la frontière entre le réseau interne et les réseaux externes, et notamment les pare-feu périmétriques, les périphériques de contrôle d'accès, les réseaux invités, l'accès distant des employés et les sites de commerce électronique.

**Évaluation de l'architecture de sécurité des communications unifiées**

Les communications unifiées constituent une application métier essentielle. Toute faiblesse sous-jacente au niveau de la sécurité de vos communications unifiées risque de vous exposer à des brèches de sécurité diverses, et notamment à des fraudes sur les appels (toll fraud), à des écoutes illicites, à du spam vocal et à des attaques par déni de service. Cette évaluation examine la sécurité utilisée pour protéger non seulement votre environnement de communications unifiées, mais aussi le réseau de données sous-jacent qui achemine vos communications. Cela inclut l'infrastructure de routage et de commutation, les applications, les serveurs et les points de terminaison requis pour générer et traiter vos communications.

**Évaluation de l'architecture de sécurité sans fil**

L'interception, les points d'accès non autorisés, les clés de cryptage faibles et les attaques par déni de service peuvent cibler votre infrastructure LAN sans fil (WLAN). Bien que les LAN sans fil génèrent des gains importants en termes de productivité, ils peuvent représenter, s'ils ne sont pas correctement configurés, un des emplacements les plus aisément exploitables de l'infrastructure. Un déploiement et une configuration appropriés de votre WLAN permettent de sécuriser votre infrastructure sans fil et ainsi de protéger vos données confidentielles et d'accroître la disponibilité. Cette évaluation examine l'architecture de sécurité qui protège l'infrastructure sans fil et associée, et notamment les contrôleurs, points accès et clients WLAN locaux et invités.

**Évaluation de l'architecture de sécurité du centre de données**

Même si les serveurs internes et les hôtes de centres de données contiennent des informations stratégiques généralement consultables par des utilisateurs approuvés, la sécurité interne reste une préoccupation majeure. Sécuriser de façon appropriée votre centre de données le protège contre les attaques internes et lui fournir un niveau de protection supplémentaire en cas d'intrusion d'un attaquant externe au sein de votre infrastructure. Cette évaluation analyse les principaux composants et technologies du centre de données, et notamment le réseau de stockage, la batterie de serveurs, l'agrégation de services, le cœur, la distribution, le contrôle d'accès et la

virtualisation des hôtes, afin de vous permettre d'utiliser pleinement et de façon sécurisée votre équipement de centre de données.

**Évaluation de l'architecture de sécurité des points de terminaison**

Les serveurs d'applications et les périphériques d'utilisateur final sont exposés à des menaces extrêmement sophistiquées, allant de courriers indésirables affectant la productivité à des attaques sociales exploitant la nature humaine. La sécurisation des périphériques d'extrémité est un élément-clé de la sécurité globale de votre infrastructure. Cette évaluation analyse l'architecture de sécurité qui protège les hôtes et les points de terminaison en dehors du centre de données, et notamment les ordinateurs portables, ordinateurs de bureau, serveurs et autres périphériques connectés à l'infrastructure.

**Évaluation des règles de pare-feu**

Il peut s'avérer ardu de configurer votre infrastructure de façon à compartimenter les comportements anormaux, en contrôler l'accès et les détecter. Mais il peut être encore plus difficile de maintenir la configuration à jour alors que l'infrastructure évolue pour prendre en charge de nouveaux services et applications, des acquisitions ou des mises à niveau, et pour se défendre contre de nouvelles menaces. Cette évaluation comprend une analyse approfondie des règles de vos périphériques de contrôle d'accès. L'analyse est encore plus intéressante lorsqu'elle est associée à d'autres évaluations qui examinent l'architecture de sécurité d'un autre domaine fonctionnel.

**Évaluation de l'architecture de sécurité physique**

Contrôler l'accès physique à votre installation est un composant-clé de la sécurité globale de votre infrastructure et de vos informations confidentielles. Si des intrus parviennent à accéder à votre infrastructure, ils sont en mesure d'installer des portes dérobées, des enregistreurs de frappes clavier, des logiciels permettant de contacter leurs auteurs et des points d'accès non autorisés, ou encore de compromettre d'autres mesures de sécurité déployées. Cette évaluation couvre les contrôles liés au périmètre et aux parties internes du bâtiment ou campus, à la surveillance de périphériques, aux capteurs environnementaux, aux communications et à l'éclairage.

## Pourquoi choisir les services Cisco ?

Les services Cisco développent des réseaux et des applications permettant une collaboration plus efficace entre les personnes qui les utilisent. Dans un monde exigeant une meilleure intégration des individus, des informations et des idées, le réseau et l'infrastructure liée deviennent une plate-forme stratégique. L'infrastructure informatique fonctionne mieux lorsque les services, associés aux produits, créent des solutions adaptées aux besoins et aux opportunités des entreprises. L'approche exclusive de Cisco prenant en compte le cycle de vie des services (Cisco Lifecycle Services) définit les activités requises à chaque phase du cycle de vie informatique pour offrir un service d'une qualité irréprochable. Grâce à une méthodologie fondée sur la collaboration et alliant les forces de Cisco, de son réseau de partenaires expérimentés et de ses clients, nous pouvons atteindre d'excellents résultats.

## Disponibilité et commandes

Le service Cisco Security Architecture Assessment Service (Service d'évaluation de l'architecture de sécurité) est disponible dans le monde entier via Cisco et ses partenaires. Les détails peuvent varier d’une zone géographique à une autre.

## Informations complémentaires

Pour plus d'informations sur les services de sécurité Cisco, visitez le site http://www.cisco.com/go/services/security ou contactez votre représentant local.

## Services Cisco

Making Networks Work.
Better Together.

**Siège social aux États-Unis**
Cisco Systems, Inc.
San Jose, Californie

**Siège social en Asie**
Cisco Systems (USA) Pte. Ltd.
Singapour

**Siège social en Europe**
Cisco Systems International BV
Amsterdam, Pays-Bas

Cisco dispose de plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site Web de Cisco à l'adresse www.cisco.com/go/offices.



Imprimé aux États-Unis C78-523857-01 06/09