HP Enterprise Security Partnership Service

Une solution d'assistance complète et collaborative pour la gestion de la sécurité, s'adressant aux organisations devant assurer la sécurité et l'intégrité de leurs infrastructures informatiques, ainsi que le maintien de leur réputation, de leur assise financière ou de leur crédibilité sur le marché

La mise en œuvre et le maintien de la sécurité d'un environnement informatique nécessite des investissements constants et un réel engagement de la part des différents intervenants. La solution HP Enterprise Security Partnership Service (ESP) vous permet de profiter au mieux des avantages de cet engagement en vous proposant un ensemble de services et de technologies avancées contribuant à l'optimisation de la sécurité des infrastructures informatiques et des informations.

Cette offre de services associe le savoir-faire et les technologies de HP en matière de sécurité aux fonctions de sécurité de Symantec™. Ensemble, nous ferons en sorte d'optimiser la disponibilité et l'intégrité de votre infrastructure informatique en tant qu'élément déterminant pour votre activité.

La solution HP ESP est mis en œuvre par une équipe de spécialistes HP et Symantec qui travailleront conjointement avec vos ressources internes. Cette collaboration contribuera à améliorer l'efficacité de votre équipe de sécurité et à renforcer la gestion et les contrôles de sécurité existants. Ce service a pour objectif de vous aider à limiter les interruptions de l'activité de votre entreprise en réduisant le nombre et l'impact d'incidents de sécurité, d'où une diminution des coûts de fonctionnement. L'équipe HP – Symantec vous proposera une solution HP ESP personnalisée et adaptée à vos besoins spécifiques.

Vous bénéficierez notamment des avantages suivants :

- Des informations, analyses et conseils pointus sur les menaces affectant la sécurité
- Une surveillance et des contrôles 24 h/24, 7j/7
- Rapidité des interventions et de la gestion des incidents
- Assistance et prise en charge en permanence des tâches de gestion de la sécurité
- Identification des risques d'exposition et des vulnérabilités face aux menaces existantes affectant la sécurité
- Mise à disposition de mesures d'atténuation aux fins de limiter les risques encourus par votre entreprise
- Fourniture d'une immunisation proactive via HP Active Countermeasures
- Elaboration et mise en œuvre d'un plan d'amélioration permanente de la sécurité

Ce service permettra d'obtenir une infrastructure informatique plus sécurisée, mieux gérée et d'une adaptabilité accrue, ainsi que des services optimisés pour votre activité. Le nombre d'incidents de sécurité et d'interruptions de service allant diminuant, vous serez en mesure de réduire vos frais et de profiter au maximum des avantages d'une infrastructure informatique plus fiable et plus sécurisée pour votre entreprise et vos activités.

symantec.

invent

La solution HP ESP s'appuie sur des principes de gestion de la sécurité informatique conformes aux normes de l'industrie ; elle vous permet d'appréhender plus efficacement les questions liées aux personnes, aux processus et aux technologies et de garantir la fourniture de services informatiques sécurisés pour votre entreprise.

Un responsable de compte nommé (CSM, Client Service Manager) de HP sera chargé de la coordination d'une équipe de consultants et d'analystes HP et Symantec tant sur site qu'à distance. L'objectif premier de cette équipe sera de vous permettre d'atteindre et de maintenir les niveaux de sécurité escomptés pour votre infrastructure informatique. L'équipe HP vous aidera à gérer les vulnérabilités technologiques, à améliorer et maintenir vos processus de gestion de la sécurité et à développer vos capacités en matière de gestion des utilisateurs. Cette approche holistique est primordiale pour parer au large spectre de menaces affectant la sécurité et aux risques associés auxquels les entreprises sont confrontées de nos jours.

Un consultant BCC (Business Critical Consultant) de HP sera désigné d'une part pour vous conseiller sur les améliorations et les bonnes pratiques en matière de sécurité, afin d'améliorer et de maintenir votre niveau de sécurité, et d'autre part pour vous aider à répondre à l'évolution des besoins de votre entreprise.

L'équipe HP s'appliquera d'abord à établir des relations de travail étroites avec votre personnel informatique. Avec lui, l'équipe HP procédera à une analyse approfondie pour identifier les domaines susceptibles de nuire à la sécurité de votre infrastructure informatique et à la qualité de vos services. Cette première évaluation nous permettra de cerner votre situation actuelle, votre système de sécurité, vos atouts et vos faiblesses, ainsi que vos objectifs en termes de sécurité de vos principaux actifs informatiques.

L'équipe HP vous fera part de ses recommandations quant à la manière de réduire ces risques et travaillera avec vous à l'élaboration d'un plan d'amélioration permanente de la sécurité et au recueil d'informations y afférentes. Ce plan permettra d'identifier les rôles, les activités, les responsabilités et les mesures visant à garantir la mise en œuvre réussie de vos services informatiques stratégiques.

L'équipe HP procédera à l'audit de votre infrastructure informatique et recueillera des informations comme sa topologie, sa configuration et ses niveaux de révision. HP les utilisera pour faire face rapidement et efficacement aux menaces informatiques et fournir des conseils spécifiques au client.

En collaboration avec votre personnel informatique et pendant toute la durée du Contrat ESP, l'équipe HP vous aidera à limiter les risques de sécurité pesant sur votre infrastructure informatique par une approche globale. Vous conviendrez avec HP d'un plan de surveillance et de mesure permettant un suivi des activités, des résultats, de la sécurité et de la qualité de service à long terme.

La nature proactive de la solution HP ESP permet de prévenir la survenue d'incidents de sécurité au niveau de l'infrastructure informatique. Toutefois, en cas d'incident, l'équipe HP vous aidera à résoudre le problème dans les plus brefs délais. Vous serez mis en relation directe avec des techniciens qualifiés qui traiteront votre dossier en priorité et vous conseilleront quant à la procédure à suivre pour résoudre votre problème.

Le contenu exact du service HP ESP et les documents y afférents seront totalement adaptés à vos besoins du point de vue de la sécurité de votre infrastructure informatique et de vos services. Il seront élaborés et documentés conjointement, sous la forme d'un Enoncé des travaux.

Avantages du service

- Réduire les risques d'indisponibilité des ressources informatiques ou de préjudice pour l'entreprise
- Limiter l'impact des failles de sécurité sur le chiffre d'affaires et sur la fidélité de vos clients
- S'assurer que les besoins spécifiques de votre entreprise en matière de sécurité des informations sont satisfaits sur le long terme
- Renforcer la confiance instaurée entre les activités informatiques et commerciales, les clients et les autres parties prenantes
- Contribuer au respect des exigences de conformité aux réglementations et certifications spécifiques du secteur
- Protéger l'entreprise dans son ensemble et s'assurer que tous les risques pesant sur la sécurité de l'infrastructure informatique sont appréhendés selon une approche exhaustive
- Armer votre organisation face aux menaces susceptibles d'affecter sa sécurité
- Une intervention efficace et proactive pour contrer les menaces affectant la sécurité informatique, grâce à la solution HP Active Countermeasures ; celle-ci permet d'identifier et de cibler les vulnérabilités prédominantes, de mettre en œuvre des mesures correctives de manière proactive et de veiller à appliquer immédiatement les mesures en question au niveau des systèmes vulnérables, avant la survenue d'une attaque. Cette démarche contraste avec une approche réactive traditionnelle lorsque l'infrastructure informatique fait déjà l'objet d'attaques et est probablement affectée.
- Rechercher et surveiller les systèmes informatiques qui ne sont pas conformes aux règles de sécurité informatique d'entreprise et qui présentent par conséquent un risque pour l'entreprise
- Définir les bonnes pratiques afin d'obtenir une infrastructure informatique sécurisée et bien gérée

Principales caractéristiques du service

Equipe d'assistance clientèle HP (voir Tableau 1)

- Responsable de compte nommé (CSM, Client Service Manager)
- Désignation d'un consultant BCC (Business Critical Consultant)
- Une équipe d'assistance (sur site et à distance) assurant la fourniture des services HP sous-jacents (par exemple, Proactive Service ou Critical Service) achetés par le client, les services décrits dans l'Enoncé des travaux élaboré conjointement et des ressources spécifiques intégrées à l'ESP
- Centre de surveillance SOC (Security Operations Center) de Symantec – composé d'ingénieurs et d'analystes ; spécialistes en sécurité

Surveillance de la sécurité et gestion des incidents en temps réel (voir Tableau 2)

Principales caractéristiques :
- Surveillance en temps réel de la fiabilité des infrastructures de défense et de sécurité telles que convenues et définies dans l'Enoncé des travaux
- Analyse de la corrélation des événements, identification des vulnérabilités et des risques
- Recommandations en matière d'actions correctrices permettant d'atténuer les risques pour la sécurité informatique
- Recueil et fourniture d'informations sur les menaces et tendances nouvelles et émergentes en matière de sécurité informatique
- Assistance et prise en charge en matière de gestion des incidents de sécurité informatique
  - Identification des incidents urgents
  - Assistance en matière d'intervention d'urgence en cas d'attaques, notamment le déploiement des actions correctrices recommandées

Options :
- Surveillance des périphériques réseau du client
- Gestion à distance de l'infrastructure de défense du client

Prise en charge permanente de la gestion de la sécurité (voir Tableau 3)

Principales caractéristiques :
- Elaboration et adoption collaboratives d'un plan de support personnalisé (PSP)
- Comptes-rendus réguliers et au cas par cas sur les vulnérabilités et les risques, ainsi que les actions correctrices recommandées
- Comptes-rendus réguliers sur les événements et incidents, les actions entreprises, l'état des menaces/alertes, l'application de correctifs, etc.
- Identification des exceptions en matière de politiques de sécurité et comptes-rendus y afférents
- Assistance et conseils en matière de correctifs de sécurité
- Conseils sur l'incidence des changements planifiés sur la sécurité via le recours à des consultants
- Assistance à la gestion des actifs
  - Audit de l'infrastructure informatique du client
  - Outils automatisés fournissant des données sur les actifs et la configuration à des fins de prise en charge de la gestion de la configuration
- Analyse des causes des incidents de sécurité informatique recensés
- HP Active Countermeasures
  - Immunisations proactives contre les nouvelles vulnérabilités
  - Recommandations en matière de mise en œuvre

Options :
- Support des équipements multimarque
  - Support du matériel
  - Support des logiciels
  - Support des périphériques de sécurité et des logiciels dédiés
- Gestion des fournisseurs
- Recueil d'informations sur la topologie, la configuration et les niveaux de révision de l'infrastructure informatique du client
- Gestion de la documentation relative à la topologie, à la configuration et aux niveaux de révision de l'infrastructure informatique du client

Proactivité de la planification et de l'amélioration de la sécurité (voir Tableau 4)

Principales caractéristiques :
- Evaluations initiales et annuelles de la sécurité, notamment la recherche et l'analyse des éléments suivants :
  - Positionnement actuel de l'infrastructure informatique en termes de sécurité
  - Etat général de l'infrastructure informatique en termes de sécurité
  - Forces et faiblesses de la sécurité informatique
  - Objectifs en matière de sécurité informatique concernant la sécurité des actifs clés
  - Evaluation des risques en matière de sécurité informatique
- Plan d'amélioration permanente de la sécurité de l'entreprise
  - Identification et prioritisation des mesures correctives requises/actions correctrices recommandées
  - Identification des domaines pour lesquels HP peut mettre en œuvre des mesures d'amélioration spécifiques
  - Comptes-rendus réguliers sur l'évolution de la situation
  - Réévaluations régulières des risques
- Le cas échéant, réactualisation du plan d'amélioration de la sécurité de l'entreprise
- Recherche régulière et à distance de vulnérabilités
- Conseils sur les règles et procédures de sécurité et sur les bonnes pratiques ISMS en matière de sécurité via le recours à des consultants
- Conseils quant à la manière de prendre en charge et d'améliorer la gestion de la sécurité et les interventions y afférentes
- Conseils sur les menaces émergentes et sur les réponses possibles/actions correctrices recommandées
- Assistance à la mise en conformité technique

Options :
- Mise en œuvre des actions correctrices recommandées en tant que partie intégrante des activités d'amélioration permanentes
- Tests d'intrusion interne et externe
- Contrôle des personnes, des procédures et des technologies suite à un incident de sécurité grave afin d'identifier des améliorations possibles

Spécifications
Tableau 1. Equipe d'assistance clientèle HP

Caractéristique ou service	Description
Responsable de compte nommé (CSM, Client Service Manager)	Un responsable de compte nommé HP est désigné comme interlocuteur privilégié du client ; il veille à ce que le service HP ESP soit correctement coordonné et intégré aux processus informatiques du client. En collaboration avec les équipes de gestion des services et de la sécurité informatiques du client, le CSM veille à ce que l'ensemble des autres membres de l'équipe d'assistance HP soient bien informés des objectifs commerciaux des services et processus informatiques stratégiques du client. Les responsabilités et prérogatives spécifiques du responsable de compte nommé sont déterminées avec soin afin de prendre en charge les services informatiques stratégiques et les objectifs commerciaux du client. En outre, elles sont convenues et répertoriées conjointement dans le plan de support personnalisé (PSP). Pour aider le client à atteindre ses objectifs commerciaux, le responsable de compte nommé procède à des contrôles réguliers du service HP ESP, planifie les interventions de l'équipe d'assistance HP, fournit des analyses des données et des comptes-rendus adaptés, gère des projets spécifiques et participe à des réunions en interne, le cas échéant. Ces activités seront menées à bien grâce à des outils de recueil des données à distance, conformément au PSP et au travers d'un ensemble de réunions sur site et de téléconférences planifiées conjointement. Le responsable de compte nommé de HP est chargé d'établir de bonnes relations avec l'équipe d'assistance HP et les principaux membres des équipes ITSM et de sécurité informatique du client.
Consultant BCC (Business Critical Consultant)	Expert en sécurité, le consultant BCC de HP sera l'interlocuteur privilégié du client en cas de problèmes liés aux processus ou aux technologies susceptibles d'avoir une incidence sur la sécurité ou l'intégrité des services informatiques stratégiques. Collaborant étroitement avec le personnel technique et les responsables informatiques du client, le consultant BCC fait figure de guide pour le maintien d'un environnement informatique sécurisé. Au début du contrat ESP, le consultant BCC procède à une première évaluation complète de la sécurité et des processus de gestion de la sécurité de l'infrastructure informatique prenant en charge les services informatiques stratégiques du client. Une analyse exhaustive des risques susceptibles d'affecter la sécurité et l'intégrité des services informatiques du client est réalisée et mise en adéquation avec les bonnes pratiques de l'industrie. Au vu de ces résultats, le consultant BCC, conjointement avec le client, élabore un plan détaillé d'amélioration permanente de la sécurité de l'entreprise (comme décrit dans le Tableau 4) afin d'appréhender toutes les zones d'exposition identifiées et d'aider le client à améliorer continuellement la sécurité et l'intégrité des informations, ainsi que la qualité de service. Disponible pendant toute la durée du contrat, le consultant BCC analyse les risques potentiels et recommande des méthodes en vue de réduire les risques en question et d'améliorer la sécurité informatique et le niveau de service du client. Les responsabilités et prestations spécifiques du consultant BCC sont déterminées avec soin afin de prendre en charge les services informatiques stratégiques et les objectifs commerciaux du client. En outre, elles sont convenues et répertoriées conjointement dans le PSP.
Equipe d'assistance	Le responsable de compte nommé forme et dirige une équipe d'assistance HP composée de l'ensemble du personnel de HP et de ses partenaires, assistant le client en vertu du présent contrat. Cette équipe d'assistance couvre l'ensemble des zones géographiques concernées par le service HP ESP. Le responsable de compte nommé coordonne l'ensemble des activités d'assistance et veille à ce que les membres de l'équipe HP soient informés des différentes interrelations entre l'infrastructure du client et les composants technologiques pris en charge. Pour ce faire, le responsable du service clients utilise un référentiel d'informations électroniques permettant à l'ensemble des membres de l'équipe d'assistance HP d'être constamment informé de tout incident exceptionnel, des activités proactives, ainsi que des services informatiques stratégiques du client et des objectifs commerciaux y afférents.

Spécifications
Tableau 2. Surveillance de la sécurité et gestion des incidents en temps réel

Caractéristique ou service	Description
Principales caractéristiques	
Surveillance de la sécurité en temps réel	HP et ses partenaires procèdent au suivi et à l'analyse des données relatives aux périphériques de sécurité du client en vue de détecter d'éventuelles activités malveillantes et d'y remédier. Les données de sécurité sont recueillies à partir des périphériques du client, converties dans un format standard et stockées dans une base de données client dédiée. HP effectue une analyse en temps réel des données de sécurité afin de détecter les attaques en cours.
Analyse de la corrélation des événements et recommandations d'actions correctrices	Les analystes de la sécurité examineront les attaques dans leur intégralité et associeront les activités de même nature survenues en d'autres points de l'infrastructure informatique du client. Par exemple, le contrôle des activités d'un service effectué avec un pare-feu d'une certaine marque pourra être mis en corrélation avec une activité similaire détectée par d'autres pare-feu, fournissant ainsi une vue complète de toute une suite d'attaques. Les événements associés seront alors passés en revue et explorés par des analystes de la sécurité. Des actions correctrices visant à atténuer les risques identifiés seront élaborées et diffusées. Des recommandations d'actions correctrices seront disponibles en temps réel en cas de situations d'urgence ou d'incidents graves.
Fourniture d'informations sur les menaces et tendances nouvelles et émergentes en matière de sécurité	Les analystes HP et Symantec poursuivront le contrôle des forums et des groupes de discussion open source afin de détecter de nouvelles menaces. En outre, les spécialistes de HP et de ses partenaires procéderont à la surveillance des activités d'un grand nombre de clients afin de détecter des situations anormales laissant présager l'émergence d'une nouvelle menace. Les analystes utiliseront les informations relatives à des événements de sécurité de même nature afin d'identifier les tendances en matière d'attaques et les menaces émergentes. Un analyste procédera à un suivi des attaques sur le long terme et conseillera son client, ce dernier pouvant ainsi prendre des mesures proactives afin de les éviter.
Prise en charge et assistance en matière de gestion des incidents de sécurité	HP identifiera les incidents urgents, et aidera ses clients à faire face immédiatement aux attaques, notamment par le déploiement d'actions correctrices. HP recommandera des actions correctrices afin de limiter les risques encourus par le client et d'aider ce dernier à gérer les incidents de sécurité informatique. HP prodiguera des conseils afin d'améliorer les procédures de gestion et de résolution des incidents de sécurité. HP fournira un modèle de procédure de fonctionnement standard pour l'escalade des événements de sécurité. Néanmoins, ce modèle pourra être personnalisé en fonction des besoins spécifiques du client. HP mettra tout en œuvre pour identifier et faire face rapidement et de manière fiable aux attaques de sécurité informatique. La méthodologie appliquée dans le cadre de la procédure de fonctionnement standard de HP inclut les étapes suivantes : 1. Diagnostic. HP confirme chaque incident et en effectue le diagnostic. 2. Publication des résultats et recommandations. Après avoir procédé au diagnostic et à l'évaluation de l'incident, HP documente les résultats, fournit des exemples et fait part de ses recommandations à des fins d'atténuation. 3. Notification des incidents. HP envoie par e-mail les informations relatives à l'incident à chaque contact figurant dans son carnet d'adresses. La procédure d'escalade standard s'organise en quatre niveaux comme indiqué ci-dessous. a. Informatif : Les analyses procéderont à l'examen des incidents de sécurité potentiels détectés sur les périphériques sous surveillance et en aviseront le client à intervalles réguliers. b. Avertissement : Via une interface client sécurisée, les analystes transmettront un descriptif, des explications et des recommandations en vue de faire face à des activités potentiellement malveillantes. c. Critique : Les analystes fourniront une notification immédiate décrivant l'entité malveillante qui est parvenue à se connecter à un système protégé. d. Urgence : L'analyste contacte le client par téléphone s'il soupçonne une atteinte au système sous surveillance. 4. Procédure d'escalade relative aux incidents graves (Critique et Urgence). Tout incident jugé critique (ou pire) donnera lieu à une procédure d'escalade transmise oralement au client dans le cadre de la procédure d'escalade convenue. Le cas échéant, HP fournira des conseils et une assistance en temps réel moyennant un coût supplémentaire afin de permettre au client de déployer des actions correctrices visant à supprimer ou limiter l'impact d'une attaque. En cas d'incidents moins graves, les actions correctrices proposées feront l'objet d'un examen puis seront classées par ordre de priorité, permettant ainsi au client d'atténuer rapidement les menaces présentant le risque le plus élevé pour l'entreprise.
Options :	
Surveillance des périphériques réseau du client	HP procédera à la surveillance des périphériques réseau à des fins de détection et de gestion des périphériques inaccessibles ou déconnectés.
Gestion à distance de l'infrastructure de défense du client	HP assurera la gestion et l'entretien des périphériques de sécurité du client en recourant aux normes établies en matière de bonnes pratiques, de configuration et de gestion des performances et en utilisant des procédures garantissant la conformité constan.

Spécifications
Tableau 3. Prise en charge permanente de la gestion de la sécurité

Caractéristique ou service	Description
Principales caractéristiques	
Plan de support personnalisé (PSP)	Le plan de support personnalisé définit l'ensemble des activités et services HP ESP convenus. Il contient une liste complète du personnel de HP et de ses partenaires impliqué dans la prise en charge des services informatiques stratégiques du client, ainsi que des informations détaillées sur tout contrat d'assistance sous-jacent et sur l'implication éventuelle de tiers. Le PSP contient également une liste par site des membres du personnel du client les plus impliqués dans la gestion et la prise en charge des services informatiques. Le PSP documente la configuration de l'infrastructure informatique du client, ainsi que les personnes et les processus impliqués dans la fourniture et la prise en charge de ses services informatiques stratégiques. Lorsque cela est possible, les données sont gérées automatiquement via des outils de surveillance à distance faisant partie du service HP ESP ou de tout autre service sous-jacent de HP. L'ensemble de ces données sont disponibles via un référentiel électronique sécurisé et peuvent être consultées et réactualisées en ligne.
Assistance et conseils en matière de correctifs de sécurité	HP fournira assistance, conseils et instructions au client afin de l'aider à améliorer la planification, les tests et le déploiement des correctifs de sécurité.
Conseils sur l'incidence des changements planifiés sur la sécurité	Le consultant BCC ou tout autre membre qualifié de l'équipe d'assistance HP peut participer au groupe de réflexion sur les changements chez le client ou à tout autre forum sur les changements afin d'aider le client à comprendre et à gérer l'impact des changements proposés.
Comptes-rendus réguliers et au cas par cas sur les vulnérabilités	HP fournira régulièrement des comptes-rendus, notamment : Etat de surveillance : il s'agit d'un état comprenant une synthèse des journaux d'événement et des incidents analysés/confirmés. Tickets de surveillance : il s'agit des tickets critiques et d'urgence les plus récents. Menaces émergentes : fournit des conseils au client sur les menaces émergentes et sur la manière de se préparer à y faire face. Contamination par des vers : fournit une liste de l'ensemble des adresses IP du client qui ont été infectées par un ver pendant la période de reporting. Top 5 des analyses : fournit une liste des 5 analyses de ports les plus fréquemment effectuées sur le réseau client. Top 5 des attaques : fournit une liste des 5 attaques les plus fréquentes dont fait l'objet le système du client. Top 5 des attaquants : fournit une liste des 5 adresses IP sources les plus virulentes.
Assistance à la gestion des actifs	HP fournira des outils de diagnostic et de correspondance pour le recueil d'informations sur l'exploration et la configuration réseau via un seul point d'accès distant sécurisé. Les ingénieurs d'assistance HP fourniront une assistance à distance uniquement avec l'autorisation du client. HP se connectera au réseau du client. HP recueillera des informations sur les périphériques réseau et connectés du client et prendra en charge la gestion des changements. HP rédigera des comptes-rendus sur le contenu et la configuration du réseau, notamment une classification des périphériques et des données sur les périphériques (y compris des informations relatives aux fichiers de configuration, au matériel et aux logiciels). Les outils d'exploration seront utilisés en permanence ou selon un planning déterminé, comme convenu avec le client.
Comptes-rendus sur les incidents	HP fournira régulièrement des comptes-rendus sur les événements et les incidents, ainsi qu'un descriptif des mesures prises. HP rédigera un compte-rendu sur les aspects du niveau de sécurité actuel du client qui pourraient avoir une incidence sur les actifs informatiques stratégiques ou sur les processus commerciaux du client.
Identifier et faire un compte-rendu sur les exceptions à des règles détectées	HP planifiera et réalisera des audits réguliers de l'infrastructure informatique du client afin d'en garantir la conformité permanente et d'identifier les éléments non conformes à la politique définie du client en matière de sécurité des informations. Le client recevra un rapport détaillé sur l'état général de ses systèmes et sur les zones de non conformité. Des conseils lui seront également prodigués quant à la manière d'assurer la conformité des systèmes en question. HP procédera à un reporting et à une analyse des tendances.
Analyse des causes des incidents de sécurité	Conjointement avec l'équipe du client, HP procédera à une analyse des causes des incidents de sécurité répondant aux critères convenus, tels que définis dans l'Enoncé des travaux.
Protection proactive contre les nouvelles vulnérabilités via HP Active Countermeasures	HP procédera à un contrôle des sources d'information d'ordre public et privé, et identifiera les vulnérabilités susceptibles d'être exploitées. Dès qu'une vulnérabilité potentiellement dangereuse sera identifiée, une action correctrice sera élaborée et testée. HP Active Countermeasures identifiera formellement chaque système client vulnérable face à cette nouvelle menace. Lorsqu'il sera décidé de prendre une action correctrice "Active Countermeasure", le système "Scan Control" sera mis en œuvre au moyen de l'action correctrice en question. Lorsqu'un système s'avère vulnérable face à un ver potentiellement néfaste, une mesure d'atténuation doit être prise. Les mesures d'atténuation seront mises en œuvre conformément à la politique de sécurité du client. A l'issue des procédures de test initiales, des actions correctrices "HP Active Countermeasures" seront prises à intervalles réguliers afin de repérer les systèmes récemment connectés, objets de vulnérabilités critiques, puis de mettre en œuvre les mesures d'atténuation qui s'imposent. Les actions correctrices "HP Active Countermeasures" permettront également d'identifier et de surveiller les systèmes non conformes aux règles de sécurité ; le client sera alors informé et invité à prendre des mesures en conséquence.
Options :	
Services de support	Un niveau adéquat de service réactif et proactif sous-jacent, tel que Proactive Service ou Critical Service, sera indiqué par HP en vue de répondre aux besoins spécifiques du client. HP mettra en place une équipe d'assistance dédiée constituée de ressources disponibles 24h/24, 7j/7 pour répondre à ces besoins spécifiques, nécessitant une intervention rapide et des compétences approfondies sur les technologies spécifiées. L'équipe d'assistance HP collaborera également avec les équipes d'ingénieurs-produit afin de garantir une résolution rapide des problèmes liés aux produits. Pour répondre aux demandes de services critiques, HP fournira un accès aux ressources techniques afin d'aider à la résolution des problèmes de mise en œuvre ou de fonctionnement dans les 30 minutes suivant la demande de service critique. La demande sera honorée dans les deux heures pour les appels concernant des services non critiques.
Gestion des fournisseurs	Si nécessaire, HP procédera à la coordination et à la gestion des services de support et des mesures correctives assurés par d'autres prestataires. HP proposera un guichet unique.
Documenter la topologie, la configuration et les niveaux de révision de l'infrastructure du client	Après concertation avec le client, HP élaborera un Enoncé des travaux distinct décrivant les activités de HP visant à documenter au format convenu les normes et à décrire en détail la topologie, la configuration et les niveaux de révision de l'infrastructure du client. HP mettra ces informations à la disposition du client, et ce dans un format convenu.
Gérer la documentation de la topologie, de la configuration et des niveaux de révision de l'infrastructure du client	Après concertation avec le client, HP élaborera un Enoncé des travaux distinct décrivant les activités de HP visant à gérer la documentation détaillant la topologie, la configuration et les niveaux de révision de l'infrastructure du client.

Spécifications
Tableau 4. Proactivité de la planification et de l'amélioration de la sécurité

Caractéristique ou service	Description
Principales caractéristiques	
Evaluation annuelle de la sécurité	HP procédera à une évaluation approfondie des risques susceptibles d'affecter la sécurité de l'infrastructure informatique et du système d'information de l'entreprise du client. L'évaluation sera effectuée par le consultant BCC ; le cas échéant, des consultants senior de l'entité HP Services et des tierces parties y participeront également. L'identification des failles de sécurité s'appuie sur une évaluation des vulnérabilités, des audits et des entretiens avec les principaux acteurs en matière d'informatique et de sécurité. Les audits peuvent inclure une évaluation de la conformité aux règles et procédures de sécurité du client, des audits de configuration, ainsi qu'un contrôle sur site de la sécurité physique. Des outils automatisés peuvent être utilisés pour évaluer les vulnérabilités, la sécurité en ligne, ainsi que la conformité aux règles. A l'issue de cette évaluation, le client recevra un rapport d'analyse détaillé indiquant les forces et les faiblesses caractérisant chaque domaine des critères spécifiés par les bonnes pratiques. Une fois identifié, chaque domaine nécessitant des améliorations sera soumis par ordre de priorité pour validation et ajout dans le plan d'amélioration permanente de la sécurité de l'entreprise. L'analyse détaillée permettra également de poser les bases d'une utilisation pendant les contrôles du service ESP et les évaluations de sécurité futures, afin de mesurer efficacement les améliorations en termes de sécurité et de services.
Plan d'amélioration permanente de la sécurité de l'entreprise	Le plan d'amélioration permanente de la sécurité de l'entreprise permettra au client d'améliorer à long terme la sécurité des informations. HP procédera à une analyse exhaustive et approfondie des services informatiques critiques du client. Les résultats de cette analyse permettront d'identifier les risques encourus en matière de sécurité et d'intégrité des services. Par ailleurs, un plan d'amélioration des services sera élaboré conjointement afin de faire face à ces risques, puis mis en œuvre au travers d'un ensemble d'activités proactives menées par HP et le service informatique du client. HP veillera à la réactualisation du plan d'amélioration permanente de la sécurité de l'entreprise.
Tests de vulnérabilité à intervalles réguliers	HP fournira ce service pour les composantes de l'infrastructure informatique du client définies dans l'Enoncé des travaux et proposera les fonctions de sécurité suivantes, si nécessaire. HP contrôlera les périphériques, les bases de données et les serveurs exposés à Internet identifiés. HP fournira au client une analyse des résultats du contrôle et un rapport écrit exposant les principaux résultats, puis proposera un plan d'action à des fins de suivi. Un contrôle des vulnérabilités sera effectué tous les trimestres, sauf mention contraire.
Conseils sur les règles de sécurité, les procédures et les bonnes pratiques de sécurité ISMS	Le consultant BCC ou tout autre membre qualifié de l'équipe d'assistance HP participera, conjointement avec l'équipe de gestion de la sécurité informatique du client, à l'identification et à la gestion des risques de sécurité informatique, ainsi qu'à l'évaluation de l'incidence de tout changement proposé. Outre les conseils en matière de gestion de la sécurité prodigués par le consultant BCC dans le cadre des contrôles effectués par le service ESP, il aidera le client à contrôler, améliorer et mettre en œuvre les principaux processus ISMS afin d'aider le client à atteindre ses objectifs professionnels et à tirer parti des bonnes pratiques du secteur.
Fournir des conseils en vue d'améliorer la gestion et la résolution des incidents de sécurité	HP procédera à une analyse régulière des procédures de gestion des incidents du client et en communiquera les résultats sous forme de rapport, ainsi que des recommandations, à des fins d'amélioration, de test et de mise en œuvre.
Fournir des conseils sur les menaces émergentes et sur les réponses possibles / actions correctrices possibles	HP rédigera des comptes-rendus réguliers et au cas par cas sur les menaces de sécurité émergentes et les tendances identifiées laissant présager une menace pour l'infrastructure informatique du client. Par ailleurs, HP communiquera des stratégies et des mesures d'amélioration pour atténuer les risques associés.
Assistance à la mise en conformité technique	Le consultant BCC ou tout autre membre qualifié de l'équipe d'assistance HP participera, conjointement avec l'équipe de gestion de la sécurité informatique du client, à l'identification et à la gestion des problèmes de conformité technique et des risques pour la sécurité associés. Il aidera le client à contrôler et à améliorer la conformité technique afin de lui permettre de satisfaire aux exigences de conformité de sa politique et de ses pratiques en matière de sécurité.
Options :	
Mise en œuvre des actions correctrices	HP mettra en œuvre les recommandations et les actions correctrices résultant des mesures d'amélioration permanentes décrites dans le présent document.
Tests d'intrusion interne et externe	Si nécessaire, HP fournira des services de tests d'intrusion interne et externe. Parmi les périphériques soumis aux tests d'intrusion peuvent figurer des périphériques réseau tels que les routeurs et les commutateurs, les serveurs d'infrastructure centralisée et des applications telles que la messagerie électronique, les serveurs d'application, les pare-feu et les périphériques IDS. Par ailleurs, des méthodes telles que l'ingénierie sociale peuvent être déployées pour tester la prise de conscience et la vulnérabilité du personnel du client, ainsi que la culture globale de l'organisation en matière de sécurité.
Analyse des interruptions de service	Le responsable de compte nommé et le consultant BCC procéderont à l'examen d'un certain nombre d'interruptions de service dues aux failles de sécurité informatique. Ils s'efforceront d'identifier les personnes, procédures ou technologies au sein de l'infrastructure informatique du client et au niveau de la mise en œuvre de la gestion de la sécurité susceptibles d'avoir provoqué ou contribué à une interruption de service non planifiée. Les résultats des analyses des interruptions de service viendront enrichir le processus de planification des améliorations du service.

Prérequis

Pour que HP puisse être en mesure de remplir avec succès ses obligations dans le cadre du Contrat ESP, un niveau adéquat de service proactif et réactif sous-jacent doit être précisé par HP.

Responsabilités du Client

Le client devra remplir l'ensemble de ses obligations, définies, le cas échéant, dans l'Enoncé des travaux convenu.

Enoncé des travaux

Les activités à réaliser dans le cadre de l'ESP varieront en fonction des besoins spécifiques du client. L'Enoncé des travaux convenu énumérera les actions spécifiques à réaliser par chacune des parties dans le cadre dudit Contrat. Le cas échéant, l'Enoncé des travaux fera mention du coût des services proposés au client par HP. L'Enoncé des travaux devra être daté et signé par HP et par le client avant l'utilisation du service HP ESP.

Dispositions générales

- Les modifications apportées à l'Enoncé des travaux signé n'entreront en vigueur que si elles ont été statuées par écrit et signées par chacune des parties.
- A la demande du client, toute tâche, y compris les fonctionnalités HP ESP en option, qui ne sera pas explicitement mentionnée dans l'Enoncé des travaux en vigueur, sera effectuée aux tarifs en vigueur de HP, tels que déterminés par HP Services.

Pour plus d'informations

Pour plus d'informations sur le service HP Enterprise Security Partnership ou sur tout autre service HP, contactez votre ingénieur commercial ou consultez notre site Web à l'adresse suivante : **www.hp.com/fr/services**

5983-2856FRE. Octobre 2005