Catalogue des services professionnels Splunk

Ce catalogue des services professionnels Splunk est fourni à titre informatif seulement et Cisco et le Client discuteront et se mettront d'accord sur les détails des services à fournir pendant la durée des services ainsi que sur toute limitation ou condition préalable (le cas échéant) associée à la prestation de services (désactivé)

Nom de l'activité	Description de l'activité
Succès de la mise en œuvre de l'alerte basée sur le risque	
L'utilisation des alertes basées sur les risques (RBA) par le biais de Splunk Enterprise Security renforcera et optimisera considérablement l'efficacité de votre SOC. L'offre de réussite d'implémentation RBA de Splunk vous permet de déployer, d'adopter et de créer de la valeur plus rapidement grâce à des règles standardisées en matière de risque et d'incident de risque, comme base pour bâtir une entreprise plus résiliente avec Splunk. Si vous utilisez déjà le système d'orchestration, d'automatisation et de réponse pour la sécurité (SOAR) de Splunk ou si vous êtes en train de le mettre en œuvre, Splunk a élaboré un ensemble de directives pour les risques notables, qui sera déployé avec Splunk SOAR, et spécialement conçu pour élargir et trier les alertes générées par le biais de la RBA méthodologie qui permet à votre équipe de travailler plus efficacement et de répondre plus rapidement aux alertes.	
Services	• **Atelier et découverte de la RBA** • **Élaborer et configurer des règles de gestion des risques et des incidents** • **Règles de risque et de risque d'incident configurées** • **Cadre du modificateur de risque** • **Feuille de route de maturation de la RBA** • **Runbooks opérationnels de la RBA** • **Transfert des connaissances avec l'équipe de sécurité** • **Implémenter et configurer le guide de stratégies pour les risques notables SOAR (le cas échéant)**
Atelier de développement de scénario de sécurité	
Que vous travailliez sur un déploiement initial ou sur la maturation de votre surveillance de la sécurité, l'atelier de développement de scénario de sécurité de Splunk Enterprise peut vous aider. Cet atelier vous aide à accroître l'efficacité de votre surveillance de la sécurité, à identifier les moyens d'améliorer votre posture de sécurité et à affiner votre stratégie de surveillance pour mieux la faire correspondre aux priorités de votre entreprise. Nos experts aident à identifier et à personnaliser les requêtes de sécurité (scénario) afin de maximiser les opportunités d'améliorer votre posture de sécurité, de s'aligner sur les besoins de votre entreprise et sur les priorités en matière de risques.	
Services	• **Atelier de développement de scénario**

Évaluation du remplacement du gestionnaire d'informations et d'événements de sécurité (SIEM)	
Nos conseillers prennent en charge le remplacement des anciens produits SIEM dans le monde entier et sont prêts à assurer votre remplacement. Nous avons mis au point un cadre permettant d'identifier les étapes critiques et les calendriers des phases importantes d'un projet de remplacement. Dans le cadre de notre atelier d'implémentation du remplacement, les clients travailleront avec nous pour élaborer un plan de migration personnalisé.	
Services	• **Identifier les scénarios à implémenter dans votre nouvel environnement** • **Élaborer un plan d'alimentation en données pour le double environnement** • **Évaluer les sources de données et mettre en correspondance les exigences en matière de données et les scénarios** • **Fournir une recommandation sur l'architecture du réseau du client pour le nouvel environnement Splunk** • **Évaluer les besoins d'intégration sur mesure (flux de travail, billetterie, etc.)** • **Planification de l'intégration pour les instances Splunk existantes qui fonctionnent déjà dans votre organisation** • **Fournir un plan de projet détaillé avec des calendriers et une estimation des efforts à fournir**
Succès des analyses de la fraude	
L'offre de service Analyses de la fraude Splunk (SFA) couvre toutes les activités nécessaires au déploiement de l'application SFA, de la préparation des données, de l'implémentation des alertes et de la création de visualisations pour les informations relatives à la fraude. Cette offre de services professionnels concerne l'implémentation de l'application Analyses de la fraude Splunk et est distincte de l'implémentation de Splunk Enterprise Security (exigence pour SFA). Nos experts peuvent effectuer les activités décrites ci-dessous pour la planification et l'implémentation des Analyses de la fraude Splunk.	
Services	• **Atelier de planification de l'implémentation :** Identifier les principaux scénarios de fraude et les sources de données applicables. Cette séance permettra de déterminer le Cette session permettra de définir le travail à effectuer pendant la durée de la mission. • **Assistance à la préparation des données :** Les experts Splunk aideront à la préparation des données, à la conformité CIM et à la configuration du modèle de données applicable. • **Examen et configuration des actifs et des identités :** Les experts Splunk vous aideront à catégoriser et à hiérarchiser vos ressources et identités internes pour une meilleure fidélité et un meilleur contexte dans les alertes et les tableaux de bord configurés. • **Examen du scénario et session de réglage :** Les experts de Splunk travailleront avec vous pour passer en revue les détections et les alertes configurées afin de s'assurer qu'elles fournissent les résultats escomptés. • **Session de révision des représentations :** Les experts Splunk travailleront avec vous pour passer en revue les représentations /tableaux de bord inclus afin de s'assurer qu'ils s'affichent correctement et de les modifier si nécessaire. • **Services de configuration des alertes basées sur le risque :** Les experts Splunk s'assureront que les risques notables sont configurés et alertent comme prévu, et vous aideront à configurer et à régler, si nécessaire, les fonctions d'alerte basées sur les risques.

Succès de l'implémentation de Splunk Observability	
L'offre de réussite de l'implémentation de Splunk Observability est un service complet conçu pour garantir la réussite de votre implémentation de Splunk Observability et pour accélérer l'adoption et le délai de rentabilisation. Nos conseillers Cisco Splunk architectureront et configureront votre environnement de supervision de l'infrastructure (IM) ou de supervision du rendement des applications (APM) avec les meilleures pratiques les plus récentes, rapidement et efficacement. L'offre est disponible en plusieurs formules (petite, moyenne, large et très large) qui sont conçues pour répondre à la taille et aux objectifs de votre organisation et qui peuvent s'appliquer à la fois aux environnements simples et complexes, aidant ainsi votre organisation dans son cheminement vers la résilience.	
Services	• **Découverte et conception** – Nos experts s'engageront dans un processus de lancement avec votre équipe pour discuter des exigences commerciales et techniques actuelles, de la validation des scénarios à déployer et de la compréhension de vos technologies et de vos outils. Nous participerons à un atelier de planification de l'architecture et de l'implémentation (non incluse dans le petit pack) pour élaborer un plan d'implémentation personnalisé, comprenant les étapes, les préalables et les meilleures configurations possibles pour votre déploiement, qu'il s'agisse de Splunk IM ou de Splunk APM. • **Configurer et implémenter l'espace sans rupture** – Développez votre environnement Splunk avec un conseiller certifié Splunk en accord avec le plan d'implémentation. Pour Splunk IM, nous allons procéder à un exercice de configuration et d'automatisation de votre infrastructure et des émetteurs de service. Pour Splunk APM, nous procéderons à une instrumentation automatique ou manuelle des applications. Pour les missions plus importantes, nous organisons des ateliers sur les scénarios et trouvons de nouvelles façons de faire évoluer la résilience de votre entreprise. • **Transfert de connaissances et documentation** – Tout au long de l'engagement, nos experts travailleront avec votre équipe pour s'assurer qu'elle comprend les processus permettant de continuer à développer et à faire évoluer la capacité de votre organisation à tirer parti de Splunk IM ou APM.

Démarrage intelligent de Splunk Observability	
Services pour accélérer votre transition vers Splunk Observability, pour aider les équipes à préparer Observability en utilisant les meilleures méthodologies et les bonnes pratiques pour une adoption plus rapide de la gamme Observability. Le processus de préparation permettra aux consommateurs et à l'équipe de supervision d'aider à développer un processus plus efficace et intuitif pour aider à adopter l'outil de supervision de l'Observabilité de manière efficace, plus rapide et pour s'assurer que vous obtenez de bons résultats dès la première fois. Tirer parti des personnes, des processus et de la gamme d'Observability pour raccourcir le délai d'obtention de la valeur et maximiser l'impact sur l'entreprise. Le processus de préparation de Splunk Observability fournit des services d'experts pour vous aider à passer à Splunk Infrastructure Monitoring, Splunk Application Performance Monitoring (APM), Browser/Mobile RUM, Log Observer et Synthetic monitoring afin de répondre à vos objectifs d'entreprise. L'implémentation sera effectuée sur un échantillon d'infrastructure, de services et d'applications afin de définir les processus de préparation de démarrage intelligents personnalisés pour répondre aux exigences de votre entreprise	
Services	• Création d'un plan de préparation structuré et personnalisé, adapté à vos besoins et à vos objectifs commerciaux. • Création d'un processus et de flux de préparation normalisés et documentés en utilisant les bonnes pratiques et méthodologies. • Création de ressources détaillées en libre-service dans votre environnement pour chaque étape du processus de préparation, depuis les exigences des consommateurs jusqu'à la création d'équipes, de tableaux de bord et de détecteurs, en passant par l'introduction des données. • Exemple d'implémentation des produits d'Observability pour implémenter le processus d'accueil. • Implémentation d'un scénario personnalisé.

	• Aider les équipes de supervision et d'évaluation à intégrer les consommateurs de manière efficace et rapide afin d'obtenir un retour sur investissement plus rapide. • Augmentation de la valeur du déploiement de Splunk Observability. • Le processus de préparation peut être lié à l'utilisation de la configuration comme support de code via Terraform. • Recommandations de formation et ateliers pour les utilisateurs finaux.

Succès du remplacement de la solution de Splunk Observability

La solution de remplacement de Splunk Observability fournit des services d'experts pour vous aider à passer à Splunk Infrastructure Monitoring (IM) ou Splunk Application Performance Monitoring (APM) afin d'atteindre vos objectifs commerciaux. Démarrez votre trajectoire d'adoption vers Splunk Observability et accélérez votre transition vers Splunk IM ou APM en suivant les méthodologies de bonnes pratiques Splunk avec les experts Splunk fournissant l'expertise technique et vous guidant à travers les défis d'une solution d'observabilité remplaçant un déploiement réussi. Les solutions de remplacement sont conçues pour convenir aux petites entreprises comme aux grandes. Modulaires et extensibles, les services peuvent être personnalisés pour répondre précisément à vos besoins spécifiques.

Services	• Atelier sur l'examen de l'architecture et des solutions existantes en matière d'observabilité. • Création d'un plan de migration basé sur votre environnement, vos scénarios et vos utilisateurs finaux pour permettre un déploiement et une transition en douceur. • Assistance à la reconfiguration d'émetteurs nouveaux ou existants et de pipelines de métriques pour collecter des métriques d'infrastructure et de service pour Splunk IM. • Assistance à l'instrumentation et à la mise à jour du code de votre application et des annotations de code pour fonctionner avec Splunk APM. • Recréation du contenu existant de visualisation et d'alerte critique pour l'entreprise avec des tableaux de bord personnalisés, des détecteurs et des politiques de notification. • Assistance à la création de contenu pour les utilisateurs finaux afin de les aider à passer à la solution Splunk Observability. • Examen et configuration des bonnes pratiques en matière de sécurité et de gouvernance. • Prise en charge de la configuration en tant que code via Terraform. • Analyses avancées avec le langage de requête SignalFlow. • Recommandations de formation et ateliers pour les utilisateurs finaux.

Évaluation de la valeur de Splunk Observability

L'évaluation de la valeur de Splunk Observability fournit des services d'experts pour obtenir une valeur maximale de votre solution Splunk Observability, axée sur la reconnaissance de la valeur supplémentaire et l'amélioration de l'adoption par le biais des bonnes pratiques, ainsi que pour vous aider à réaliser la valeur requise de la solution Splunk Infrastructure Monitoring ou Splunk Application Performance Monitoring par rapport à vos objectifs d'entreprise. Les packs d'évaluation de la valeur sont dimensionnés pour convenir aux petites entreprises comme aux grandes. Modulaires et extensibles, les services peuvent être personnalisés pour répondre précisément à vos besoins spécifiques. Lors d'une évaluation de la valeur de l'observabilité, nos experts Splunk travailleront en partenariat avec vous et vous fourniront des conseils sur les bonnes pratiques pour améliorer la valeur et la compréhension de vos scénarios de l'observabilité. Le service propose l'optimisation des cas d'utilisation, l'examen de la configuration et des recommandations.

Services	• Examen de l'architecture et du déploiement actuels des produits Splunk Observability • L'examen peut porter sur l'instrumentation des mesures, l'instrumentation APM, les scénarios des graphiques et des tableaux de bord, les détecteurs, les intégrations sortantes et les flux de travail de dépannage. • Suggestions basées sur les bonnes pratiques pour améliorer la valeur des instruments actuels, des tableaux de bord, des détecteurs et des flux de travail de dépannage. • Des mises à jour sur les nouvelles caractéristiques et fonctions de la plateforme et sur la manière dont elles peuvent être utilisées pour obtenir des observations supplémentaires ou améliorer l'expérience de l'utilisateur final. • Présentation exécutive des résultats et des recommandations. • Conseils pour obtenir une valeur ajoutée en utilisant des fonctionnalités avancées telles que des conditions de détection intégrées, des analyses SignalFlow avancées ou la gestion du contenu en tant que code via Terraform. • Identification de sources de données supplémentaires et de scénario pour fournir des observations et une valeur supplémentaires. • Recommandations et conseils pour préparer des sources de données supplémentaires et mettre en œuvre de nouveaux scénarios tout en respectant les bonnes pratiques de l'industrie. • Optimisation des scénarios existants tels que la réduction du bruit excessif, les détecteurs d'erreur, l'amélioration de la lisibilité, l'optimisation des tableaux de bord et l'ajustement des métadonnées pour rendre les données que vous envoyez plus utiles et plus significatives.

Succès de la migration vers Splunk Cloud

L'offre de réussite de la migration vers le Splunk Cloud va procéder à un examen holistique de votre architecture Splunk et des meilleures pratiques de déploiement Splunk afin de déterminer le chemin de migration vers le Splunk Cloud. Nous fournissons des conseils et de l'expertise non seulement pour faire migrer votre déploiement, mais aussi pour l'optimiser pour Splunk Cloud. L'offre de réussite de la migration vers Splunk Cloud est conçue pour les clients de Splunk qui cherchent à minimiser les temps d'arrêt et le temps nécessaire pour migrer vers Splunk Cloud. En outre, cette migration s'adresse aux clients qui ont besoin de préserver leurs données historiques Splunk dans le format d'origine, qui souhaitent implémenter un déploiement Splunk selon les bonnes pratiques et qui ont déjà intégré des données et des applications personnalisées.

Services	• Les services de planification comprennent la recherche de ressources, la liste de contrôle de la plateforme, la réunion de lancement, l'évaluation de la source de données. • Les services de livraison et d'exécution comprennent l'examen de l'architecture, l'optimisation pour le nuage, l'approvisionnement du nuage, le démarrage du nuage, la migration des données, la migration du contenu des clients, le découpage, la stabilisation. • Les services d'achèvement comprennent la mise au point

Succès de l'implémentation de Splunk Enterprise/Cloud

L'offre de réussite de l'implémentation de Splunk Enterprise/Cloud fournit aux nouveaux clients les bases nécessaires pour offrir des performances et de l'ampleur à leurs utilisateurs finaux. En s'appuyant sur les bonnes pratiques les plus récentes, nos conseillers accrédités Splunk, nos concepteurs de solutions et nos responsables de livraison travailleront avec vous pour implémenter le meilleur déploiement de Splunk en fonction de vos besoins.

Services	En fonction de la taille du pack acheté, les services suivants peuvent être livrés : • Les services de planification comprennent la recherche de ressources, la liste de contrôle de la plateforme, la réunion de lancement, l'évaluation des sources de données • La création d'un plan d'implémentation personnalisé décrivant l'architecture, les scénarios, les données et les critères de réussite • L'installation et la configuration d'une architecture de collecte de données Splunk conforme aux bonnes pratiques • La collecte de données dans Splunk • Discuter du modèle de stockage et de sécurité de Splunk, appliquer le modèle de sécurité aux données dans Splunk • Intégrer les points de configuration clés au contrôle de la source • Consultation pour déterminer les exigences et les critères de réussite • Compréhension des données et extraction de connaissances à partir des données comprises • Application de balises et extension des conventions d'appellation pour une recherche plus aisée • Recherche de données à partir d'un emplacement central, création d'alertes basées sur des données importantes • Création de rapports et d'analyses approfondies pour les opérations, la sécurité, l'analyse commerciale et les dirigeants • Installation d'une application SplunkBase ou création d'une application personnalisée

Vérification de l'optimisation

Lorsque vous préparez des données et des utilisateurs dans votre environnement Splunk, il est utile de jeter un coup d'œil sous le capot pour s'assurer que vos recherches et vos tableaux de bord fonctionnent toujours à leur rendement maximal. Que vous vous prépariez à une mise à niveau, à une réorganisation, à une mise à l'échelle ou que vous n'obteniez tout simplement pas la vitesse attendue pour les recherches et les tableaux de bord, cette offre peut vous aider. Cette offre comprend un examen de l'architecture, des configurations, des objets de connaissance, de la gouvernance des données et des scénarios. En s'appuyant sur les bonnes pratiques, nos experts Splunk s'assureront que vos utilisateurs et administrateurs bénéficient de l'expérience qu'ils attendent.

Services	• Révision de l'architecture et des configurations Splunk (indexeurs, têtes de recherche, points de configuration) • Évaluation des performances de haut niveau (mesures des performances de Splunk, recherches lentes ou ignorées, goulots d'étranglement) • Évaluation approfondie des sources de données (configurations d'entrée, extractions de champs, consultations, Boutique KV et modèles de données) • Vérifier les applications déployées / les modules techniques et de leur configuration • Vérifier les recherches existantes afin d'identifier les recherches inefficaces et fournir des recommandations • Examiner la capacité de recherche et d'indexation par rapport aux besoins actuels et prévus • Examiner les problèmes connus ou identifiés en matière d'environnement, de performance ou de stabilité • Identifier les fonctionnalités qui pourraient être utilisées pour optimiser l'expérience du client • Examiner un sous-ensemble défini de tableaux de bord existants - fournir au client un commentaire et les bonnes pratiques • Vérifier la rétention des données et les paramètres de sécurité, en examinant la propriété des sources de données et les autorisations en place

Succès de l'implémentation de Splunk Enterprise Security	
L'offre de réussite de l'implémentation de Splunk Enterprise Security (ES) se décline en trois tailles - basique, standard et premium - pour fournir les capacités qui optimiseront l'implémentation et la TTV au sein de votre environnement. **Offre basique** - L'offre basique est conçue pour les clients disposant de plus de ressources internes dédiées au projet Splunk. Les administrateurs et utilisateurs internes de Splunk recevront une formation informelle de la part du consultant accrédité Splunk et accompliront les tâches restantes une fois que les services professionnels Splunk auront terminé leur travail. **Offre standard** - Pour les clients qui recherchent plus de support lors de l'installation initiale, mais qui sont convaincus que la maintenance et l'optimisation continues de Splunk seront bien gérées par les ressources internes, vous pouvez vous appuyer sur les services proposés dans Basique avec notre offre standard. **Offre Premium** - Cette offre est destinée aux clients qui reconnaissent l'opportunité d'une valeur commerciale supplémentaire au-delà de l'ensemble des scénarios initiaux. L'offre Premium comprend des services supplémentaires par rapport à l'offre Standard, tels qu'une assistance permanente en matière d'architecture, d'ateliers et d'optimisation, ainsi qu'un renforcement du personnel pour répondre aux besoins supplémentaires en matière de scénario et de résultats.	
Services	• Planification : Atelier avec un concepteur de solutions afin d'élaborer un plan de scénario. • Installation : Déployer Splunk Enterprise dans votre environnement; Intégrer sept ou neuf sources de données essentielles; Installer Splunk Enterprise Security; Déployer et optimiser 7 à 18+ scénarios (recherches par corrélation) pour votre environnement; Optimiser le contenu prêt à l'emploi. • Formation : Fournir une formation à distance pour vos administrateurs Splunk; effectuer une visite guidée des fonctionnalités ES pour votre personnel; revoir les bonnes pratiques pour l'intégration des données; revoir les bonnes pratiques pour la création de recherches de corrélation. • Coordination - Un gestionnaire de prestation vous accompagne sur la voie du succès
Succès de l'implémentation de Splunk ITSI	
Le succès de l'implémentation de Splunk IT Service Intelligence (ITSI) est conçu pour les nouvelles installations dans les environnements Splunk Cloud ou sur site. L'offre est conçue pour les clients qui découvrent Splunk IT Service Intelligence (ITSI). Cette offre de services professionnels aide les clients à configurer avec succès des éléments tels que les services, les indicateurs de performance clés, les seuils adaptatifs, la détection des anomalies, la santé prédictive des services et l'analyse des événements afin d'obtenir une meilleure visibilité et une meilleure observation de la santé de leurs services et appareils surveillés. Les packs de préparation Splunk sont dimensionnés pour convenir aux petites et grandes structures, jusqu'au niveau d'entreprise. Modulaires et extensibles, les offres préconstruites peuvent être personnalisées pour répondre précisément à vos exigences et objectifs spécifiques.	
Services	• Session de recueil des besoins - Recueillir et documenter les buts et objectifs majeurs de l'entreprise. Créer un plan pour tirer parti de l'ITSI afin d'atteindre ces objectifs. • Atelier d'identification des services - L'architecte Splunk travaillera avec les clients et les parties prenantes pour identifier, collecter, hiérarchiser et documenter les services, les exigences associées et les flux de travail. • Atelier de décomposition des services - Identifier les indicateurs clés de performance et les dépendances des services afin de superviser efficacement leur état de santé. Identifier les sources de données nécessaires et leur importance. • Préparation et validation des données - Valider la préparation correcte des sources de données nécessaires pour alimenter les indicateurs de performance clés et fournir un plan de préparation des données manquantes conformément aux bonnes pratiques de Splunk.

	• Installation et configuration de l'application IT Service Intelligence – Les services professionnels de Splunk suivront les bonnes pratiques et les méthodologies standard pour l'installation et la configuration de l'ITSI et des autres applications et modules complémentaires requis. • Atelier d'analyse des événements de l'ITSI – Recueillir les besoins et discuter des résultats souhaités. Identifier les sources de données d'alerte, les actions d'alerte et les intégrations. Élaborer un plan d'implémentation pour atteindre les objectifs.
Succès de l'implémentation de Splunk SOAR	
L'automatisation, l'orchestration et la réponse en matière de sécurité (SOAR) modifient le monde des opérations de sécurité, de la réponse aux incidents, de la gouvernance et de l'activation des informations sur les menaces. L'offre de réussite de l'implémentation Splunk SOAR a été conçue pour répondre aux besoins et à la maturité du programme de sécurité du client.	
Services	Chaque client est différent, c'est pourquoi Splunk dispose d'un modèle de dimensionnement unique pour répondre à vos besoins. Le service de base fournit les services suivants : • Réunion de lancement pour harmoniser les objectifs, les ressources et les calendriers. • Un atelier de révision de l'architecture pour identifier l'architecture Splunk SOAR validée qui répond aux besoins du client. • L'installation, la configuration de l'instance SOAR. • L'intégration de l'instance Enterprise ou Enterprise Security du client pour permettre l'échange de données entre les deux plateformes, et la configuration d'une liste initiale de 5 intégrations d'applications dans SOAR. • La mise en place de sessions de transfert de connaissances spécifiques au client pour aider à l'identification des scénarios, guides et manuels adéquats. • Le codéveloppement d'un plan d'intervention sélectionné en un ensemble pouvant aller jusqu'à 5 guides ou manuels.
Succès de l'implémentation de Splunk UBA	
Splunk User Behavior Analytics (UBA) est une solution basée sur l'apprentissage automatique qui livre les réponses dont vous avez besoin pour détecter les menaces inconnues et les comportements anormaux chez les utilisateurs, les points terminaux d'utilisateur et les applications. Il ne se concentre pas seulement sur les attaques externes, mais aussi sur la menace interne. Ses algorithmes d'apprentissage automatique produisent des résultats exploitables avec des cotes de risque et des preuves à l'appui qui renforcent les techniques existantes des analystes des Centres des opérations de sécurité (SOC) pour une action plus rapide. L'offre de réussite de l'implémentation de Splunk Professional Services UBA est conçue pour les clients qui cherchent à incorporer une solution utilisant l'apprentissage automatique et les analyses de détection d'anomalies dans leur Centre des opérations de sécurité pour prévenir, détecter et répondre aux cyberattaquants dans le paysage de la sécurité d'aujourd'hui.	
Services	Cette offre de services professionnels concerne uniquement Splunk UBA. Les activités suivantes peuvent être effectuées pour l'offre standard de Splunk UBA : • Atelier de planification de l'implémentation : Passez du temps avec un concepteur de solutions Splunk pour découvrir les exigences et personnaliser un plan de projet qui définira le travail à effectuer pendant la durée du projet. La coordination du projet et le suivi des succès sont assurés par le chef de projet Splunk. • Services de configuration : Un conseiller accrédité Splunk utilisera les bonnes pratiques pour installer Splunk UBA tout en exécutant le plan de projet. Ils s'assureront que toutes les sources de données requises par l'UBA arrivent dans l'UBA et sont normalisées correctement.

	• Sessions d'examen des scénarios : Une fois que les données sont en place pour la période de référence conseillée et que les scénarios sont activés, le conseiller rendra opérationnels et mettra au point les scénarios de Splunk UBA. • Séances de transfert de connaissances : Les services professionnels organiseront des sessions pour démontrer l'implémentation et documenter les éléments administratifs. Les meilleures pratiques seront communiquées et partagées en ce qui concerne l'administration générale de l'application.