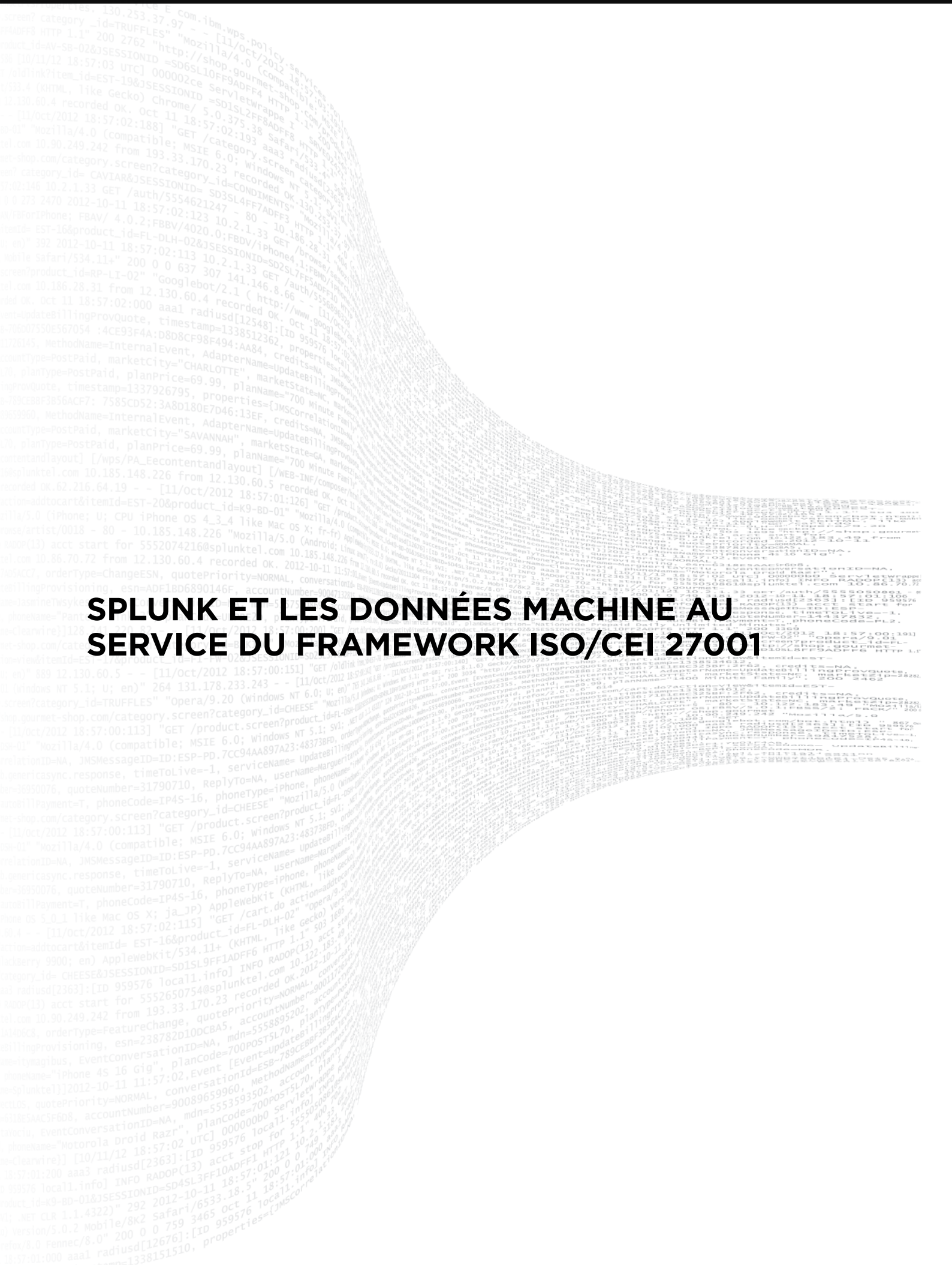
splunk>

LIVRE BLANC

SPLUNK ET LES DONNÉES MACHINE AU SERVICE DU FRAMEWORK ISO/CEI 27001



La transformation numérique, l'impératif de nouer une relation de confiance avec le client, et une palette de lois, réglementations et normes diverses contraignent les entreprises du monde entier à formaliser leurs programmes de sécurité. Pendant des années, la sécurité a été considérée par les comités de direction comme une problématique strictement technologique. Cette vision a radicalement changé au cours des dernières années : la gouvernance IT et la mise en place d'un système de gestion de la sécurité informatique (ISMS) basé sur ISO 27001 est aujourd'hui une priorité pour les entreprises.

Le Directeur de la sécurité informatique (RSSI) a pour mission de mettre au point des stratégies de sécurité alignées sur les activités du moment et celles de demain. Le RSSI est également responsable du développement et de l'exécution du programme de gestion des risques informatiques de l'entreprise. Les entreprises ont besoin d'élaborer et de mettre en place des politiques de sécurité, de nouvelles capacités – des processus de réponse aux incidents notamment – et, bien souvent, des fonctions de sécurité plus opérationnelles.

Pour y parvenir, on peut mettre en place un ensemble adapté de contrôlés basés sur les directives de la norme de sécurité des informations ISO 27002.

Splunk donne aux équipes de sécurité de toutes les tailles la possibilité d'explorer, superviser, analyser et exploiter les renseignements extraits des données machine générées par chaque réseau, système, base de données, serveur web, application et appareil connecté à Internet. Les équipes de sécurité utilisent Splunk comme facilitateur de processus et multiplicateur de force pour accomplir plus de travail en moins de temps, pour un coût inférieur et avec une précision accrue.

La plateforme Splunk offre également un bon retour sur investissement à ces équipes en leur permettant d'exploiter les données utilisées pour la conformité à d'autres fins que celle-ci. Les mêmes données machine peuvent être utiles aux équipes des opérations IT, de développement d'applications, d'analyse commerciale et d'Industrie 4.0/IoT.

Le résultat : une intelligence des opérations et de la sécurité fortement axée sur les risques pesant sur les fonctions métier stratégiques qui affectent directement les recettes, et les risques de conformité qui peuvent dégrader la réputation, la confiance des clients et le résultat final.

Découvrez ce que peut faire Splunk

Le logiciel Splunk est une plateforme big data pour les données de sécurité et les données machine qui appuie la mise en œuvre d'ISO 27002 de plusieurs façons :

- En fournissant des rapports sur les données machine comme preuves de conformité en cas de contrôle
- En protégeant les données machine contre les consultations, modifications et suppressions non autorisées, et en conservant des tracés d'audit
- En délivrant des revues quotidiennes des systèmes pour comparer les comportements aux politiques en vigueur
- En supervisant les périphériques réseau, les serveurs, les applications et les transactions dans le cadre de l'évaluation des risques opérationnels et de sécurité, à des fins de résilience des activités
- En offrant la possibilité d'effectuer des recherches des causes profondes
- En facilitant les requêtes de divulgation électronique des services émises par les autorités
- En permettant d'effectuer des enquêtes RH sur l'activité d'un employé
- En donnant au personnel de conformité un accès sur demande aux données IT
- En apportant la preuve de l'intégrité des données d'audit

Méthode de mise en œuvre :

Mythe : Il existe un ensemble précis de rapports qui assureront ma conformité.

Réalité : Les réglementations ne mentionnent généralement aucun rapport spécifique. Certains rapports peuvent appuyer des exigences spécifiques, comme l'impératif d'inspection des échecs de connexion, mais ils doivent être finement adaptés à chaque environnement. Au mieux, un ensemble de rapports standard constitue un bon point de départ. En effet, il faut savoir que la plupart des suites de rapports de conformité sont élaborés par des responsables de produits qui lisent les réglementations et tentent de deviner quels rapports pourraient être utiles. La tendance la plus récente en matière d'audit consiste à demander à un représentant de l'IT de présenter une requête ad hoc en réponse à la demande d'un contrôleur

ou à une exigence.

Chaque entreprise a sa façon de gérer le risque, et cela peut même varier d'un service à l'autre. Il faudrait donc définir des directives de sécurité des informations afin d'imposer une approche basée sur les résultats. Pour implémenter les contrôles définis dans les directives de sécurité des informations d'une entreprise au sein des cas d'usage SIEM dans la perspective d'ISO 27002, on recommande de suivre les étapes ci-dessous :

1) Examinez les directives de sécurité des informations imposées par votre entreprise et déterminez si votre SIEM peut répondre à chacune d'elle.
2) Identifiez les questions posées ainsi que les actions et voies d'escalade organisationnelles nécessaires pour y répondre.
3) Identifiez les systèmes, composants techniques et applications qui détiennent les données requises pour obtenir la réponse recherchée.
4) Collectez les données machine.
5) Explorez les données machine et trouvez les entrées qui renferment la réponse.
   a) Identifiez les normes de journalisation et vérifiez que le niveau de journalisation est correctement configuré sur les sources de données supervisées.
6) Définissez la logique de rapport requise et les enrichissements éventuellement nécessaires.
7) Rédigez la requête de recherche Splunk (ou reprenez et adaptez une requête provenant de tableaux de bord ou de rapports prédéfinis).
8) Faites le choix entre rapports réguliers et alerte en cas d'événement de sécurité en temps réel, ou optez pour les deux approches.

Les étapes 5 à 8 se font dans la plateforme Splunk en quelques minutes généralement grâce au puissant langage de recherche du logiciel, aux fonctionnalités de schémas à la volée et aux plus de 1 500 applications sur **Splunkbase** qui proposent des tableaux de bord et des rapports prédéfinis.

Consultez le tableau ci-dessous pour connaître dans le détail la façon dont les données machine et la plateforme Splunk peut appuyer vos efforts de conformité aux contrôles d'ISO 27002.

Domaines clés d'ISO 27002	Appui fourni par Splunk et les données machine
6.1.2 Séparation des tâches	La séparation des tâches peut être difficile à mettre en œuvre pour les petites entreprises. D'autres contrôles, comme les activités de supervision et la conservation de traces d'audit, doivent être envisagés. Splunk permet aux petites organisations de consigner ces suivis et de superviser les activités, puis de séparer les responsabilités au niveau des applications et des processus numériques. On peut ensuite effectuer une analyse des activités pour assurer la séparation des responsabilités entre différents individus et/ou rôles établis. Splunk Enterprise prend en charge le contrôle des accès basés sur le rôle, grâce auquel l'accès aux informations est accordé ou non selon le rôle spécifique de l'utilisateur. Les comptes utilisateur de Splunk peuvent être liés à Active Directory ou LDAP pour mettre en place l'authentification unique (SSO).
6.1.5 La sécurité de l'informations dans la gestion de projet	Splunk permet à l'équipe de projet d'explorer au plus tôt les données machine inconnues générées par un service numérique, pour identifier les risques et contrôles indispensables. Il est essentiel de comprendre ce qui est visible dans les données machine et quels types d'événements et d'actions peuvent manquer, d'identifier en quoi consiste la normalité, et de recommander les anomalies à rechercher dans le cadre de la supervision de sécurité du système de production.

Domaines clés d'ISO 27002	Appui fourni par Splunk et les données machine
6.2.1 Politique en matière d'appareils mobiles	Splunk permet de collecter les données des systèmes de gestion des appareils mobiles et de produire des rapports, mais aussi de recueillir les données des services de synchronisation du courrier électronique mobile pour identifier les enregistrements de nouveaux appareils et les mises à jour nécessaires, produire des rapports sur l'application des politiques et documenter l'exécution réussie des opérations d'effacement à distance en cas de perte ou de vol d'un téléphone.
6.2.2 Télétravail	Splunk permet aux entreprises de conserver un suivi d'audit complet de tous les composants utilisés pour des activités de télétravail, et ainsi de consigner, par exemple, les connexions par VPN, les accès aux fichiers sensibles d'un serveur via une session de terminal et les éventuelles tâches d'impression. Ces suivis permettent de savoir qui accède à quoi, quand et comment, et de créer des alertes en cas d'infraction aux politiques de sécurité.
7.1.2 Termes et conditions d'embauche	Splunk permet de tenir une liste des employés et sous-traitants qui ont signé un accord de confidentialité (NDA) et de rapprocher cette liste des logs d'accès aux informations confidentielles. On peut ensuite déclencher une alerte si une personne non autorisée accède à des données sensibles. La liste des utilisateurs peut être configurée de manière à se synchroniser automatiquement avec le système légal ou RH via tout type d'API de base de données ou d'application, pour signaler la signature ou la révocation des accords de confidentialité.
7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information	Splunk peut être utilisé pour superviser les systèmes d'e-learning afin de vérifier que les employés suivent bien les formations sur la sécurité des informations. On peut également définir des actions de réponse pour assigner des formations supplémentaires en fonction du comportement de l'utilisateur.
7.2.3 Processus disciplinaire	Splunk aide les équipes IT et de sécurité à répondre aux demandes des RH et du service juridique en cas de violation de la sécurité des informations par un employé. Elles peuvent conduire des enquêtes sur les systèmes et les réseaux pour identifier et éventuellement remplacer l'employé en cas de compromission d'un compte d'utilisateur technique.
7.2.3 Processus disciplinaire	Splunk permet également à l'équipe de gestion de la sécurité IT de mettre en place un système de récompense ou d'incitation en cas de comportement remarquable en matière de sécurité des informations, grâce à des rapports de bonne conduite. Elle peut identifier les employés qui changent de mot de passe le plus souvent ou signalent le plus d'emails de hameçonnage à la sécurité informatique.
8.1.1 Inventaire des actifs	Splunk permet de produire des listes d'actifs à partir de plusieurs systèmes, de les comparer pour en confirmer l'exactitude, d'identifier les actifs manquants puis de mettre les listes à jour. On peut ainsi extraire une liste de la base de données CMDB et la synchroniser avec le contenu d'Active Directory, les actifs inspectés par le détecteur de vulnérabilités, les requêtes DHCP et les éléments visibles dans le système de gestion de la protection des terminaux.
8.1.2 Propriété des actifs	Splunk permet aux équipes de tenir une liste des actifs incluant le responsable de chaque actif, sa classification et des notes sur les éléments à mettre à jour régulièrement dans Splunk Enterprise Security. Il est possible d'établir des tableaux de bord spécialisés pour chaque responsable d'actifs afin d'élargir la sécurité des informations et de la rendre plus accessible.
8.1.4 Restitution des actifs	Lorsqu'un employé ou un sous-traitant arrive en fin de contrat, l'entreprise doit surveiller étroitement son activité pour détecter toute copie non autorisée d'informations de valeur. Splunk peut mettre des utilisateurs sur une liste de surveillance et établir des corrélations avec les événements de copie non autorisée comme l'envoi de données sur des plateformes de stockage en ligne (Google Drive ou Dropbox par exemple), l'envoi d'emails vers des domaines privés (@gmail.com) ou l'utilisation de supports de stockage amovibles. On peut encore mener des enquêtes historiques pour détecter les copies non autorisées d'informations stratégiques qui ont été réalisées avant la fin du contrat d'un employé.

Domaines clés d'ISO 27002	Appui fourni par Splunk et les données machine
8.3.1 Gestion des supports amovibles	Splunk permet aux entreprises de recueillir directement les données des terminaux ou d'utiliser des outils de protection tiers (outils de contrôle des périphériques ou DLP). On peut superviser la copie de données vers des supports amovibles et consigner ces activités à titre de preuves. Grâce à l'identification unique des supports amovibles, on peut tracer une infection potentielle de malware en examinant, par exemple, sur quelles machines de l'environnement de l'entreprise une clé USB a été connectée. Il est également possible de retracer l'utilisation globale de la clé USB : des utilisations multiples peuvent indiquer un besoin de formation à la sécurité.
8.3.2 Mise au rebut des supports	Splunk permet de conserver un suivi d'audit et de superviser un PC de nettoyage équipé d'un logiciel de suppression, utilisé par les équipes IT pour effacer le contenu des supports de stockage au moyen de procédures normalisées.
8.3.3 Transfert physique des supports	Voir le point 8.3.1 et suivants pour valider et démontrer que les données stockées sur des supports amovibles étaient chiffrées.
9.1.1 Politique de contrôles d'accès	Splunk permet aux utilisateurs d'interroger des listes de contrôle d'accès tiers à l'aide de commandes de recherche ou d'extensions techniques, puis de stocker ces instantanés pour les présenter dans des tableaux de bord à la personne responsable des informations. Par exemple, grâce à la commande « sa-ldap search » de Splunk, on peut obtenir une liste des membres d'un groupe Active Directory autorisés à accéder à des informations confidentielles, puis stocker cette liste et produire un rapport. Il est même possible de générer ce rapport à intervalle régulier pour suivre et produire un audit de la configuration à tout moment.
9.1.1 Politique de contrôles d'accès	Avec Splunk, il est possible de recueillir les logs d'audit de n'importe quel système de gestion des applications, de l'authentification ou des identités pour tracer les opérations administratives.
9.1.2 Accès aux réseaux et aux services en réseau	Splunk permet de conserver un suivi d'audit complet de tous les composants impliqués dans l'accès au réseau ou aux services réseau. Splunk facilite la supervision de l'utilisation des services réseau et fournit des réponses aux questions du type : « qui a accédé à quoi, quand et comment ». Les administrateurs peuvent ensuite déclencher une alerte en cas d'activité non conforme à la politique de l'entreprise.
9.2.1 Enregistrement et désinscription des utilisateurs	Splunk permet de conserver un suivi d'audit des actions des utilisateurs afin de les tenir responsables de leurs actes. Des événements comme le partage de comptes d'utilisateur peuvent être détectés grâce à des recherches de corrélation prêtes à l'emploi de Splunk Enterprise Security. Les exceptions sont gérées au moyen de listes blanches.
9.2.1 Enregistrement et désinscription des utilisateurs	Splunk fait plus que permettre aux entreprises de conserver un suivi d'audit des comptes utilisateur désactivés ou supprimés. Splunk peut également enrichir les informations sur les utilisateurs en fin de contrat en puisant directement dans l'application RH ou dans le système de tickets afin de produire une alerte en cas d'échec d'un processus organisationnel ou technique ou d'omission de suppression d'un compte dans l'un des nombreux systèmes de l'entreprise.
9.2.2 Maîtrise de la gestion des accès utilisateur	Splunk permet de recueillir les données des logs d'événements auprès d'un système d'autorisation pour savoir quel administrateur a accordé à un identifiant utilisateur l'accès à un système informatique ou un service spécifique.
9.2.3 Gestion des privilèges d'accès	Splunk supervise les changements de privilèges et l'évolution des indicateurs et des escalades d'accès.
9.2.4 Gestion des informations secrètes d'authentification des utilisateurs	Splunk suit et supervise la première utilisation des comptes utilisateur, notamment pour confirmer que le mot de passe par défaut a été modifié.

Domaines clés d'ISO 27002	Appui fourni par Splunk et les données machine
9.2.5 Revue des droits d'accès utilisateur	Splunk peut interroger les applications et les services pour produire des rapports sur les accès utilisateur et fournir un rapport automatisé au responsable de l'actif concerné. Splunk peut également indiquer tout type de modification des attributs des utilisateurs par rapport à un rapport précédent.
9.2.5 Revue des droits d'accès utilisateur	Splunk peut enregistrer et signaler les modifications affectant des comptes utilisateur et documenter l'examen ou l'accès régulier à un rapport grâce à ses outils internes d'audit.
9.2.6 Suppression ou adaptation des droits d'accès	Splunk supervise le processus de suppression ou de modification des droits d'accès, par exemple lorsqu'un employé change de service ou arrive en fin de contrat. En cas d'ajout ou de suppression d'un utilisateur, Splunk peut informer les opérations IT du changement pour qu'elles puissent confirmer que la procédure était autorisée.
9.4.2 Sécuriser les procédures de connexion	Splunk facilite la supervision et la production de rapports sur les systèmes d'authentification à deux facteurs et les solutions d'authentification unique (single sign-on), et permet d'interroger un fournisseur d'identité et d'enregistrer les tentatives d'authentification.
9.4.2 Sécuriser les procédures de connexion	Splunk permet de collecter les échecs de connexion et les tentatives réussies auprès de quasiment tout type d'application, de service ou de système.
9.4.2 Sécuriser les procédures de connexion	Splunk détecte les activités de force brute grâce à différentes méthodes d'analyse, allant du simple décompte au machine learning en passant par l'établissement de valeurs de référence, et en incluant la détection des tentatives lentes.
9.4.4 Utilisation de programmes utilitaires à privilèges	L'utilisation d'utilitaires système peut être supervisée et corrélée par Splunk. Des mécanismes de détection avancée sont proposés, comme l'analyse ou la classification dynamique de groupe de pairs et la mesure de la longueur des entrées de ligne de commande.
9.4.5 Contrôle d'accès au code source des programmes	Splunk peut superviser les systèmes d'extraction et d'archivage logiciel pour contrôler les accès et assurer la séparation des équipes de développement et de QA.
10.1.2 Gestion des clés	Vous pouvez utiliser Splunk pour superviser l'infrastructure PKI et les appliances de chiffrement HSM (génération des clés, exportations, inscriptions, vérifications et révocations).
11.1.2 Contrôles physiques des accès	Splunk peut être employé pour surveiller les accès physiques aux locaux ainsi que les habitudes d'accès pour détecter les intrusions non autorisées. Les données d'Active Directory, des accès physiques et des VPN peuvent être corrélées pour détecter les intrusions de type « tail-gating » (quand une personne profite du passage d'un utilisateur autorisé pour s'introduire dans un bâtiment).
11.2.1 Emplacement et protection du matériel	Splunk peut traiter des données dans tous les formats ou presque, y compris les données des systèmes CVC des bâtiments, afin de détecter les changements de température et les menaces physiques associées. Splunk accepte et supervise les données des systèmes RFID et les informations GPS, ce qui lui permet de suivre l'utilisation des camions et des équipements (équipés de balises RFID/GPS) pour les protéger contre le vol.
11.2.2 Services généraux	Splunk recueille tous les types de données de capteurs et d'alertes de sécurité émises par les équipements des bâtiments et peut informer les équipes IT pour éviter que seule l'équipe de gestion des installations ait de la visibilité sur ces informations.
11.2.8 Matériel utilisateur laissé sans surveillance	Splunk peut superviser l'inactivité d'un hôte et notamment les données indiquant que l'économiseur d'écran est actif ou ne s'est pas lancé dans un délai spécifique.

Domaines clés d'ISO 27002	Appui fourni par Splunk et les données machine
12.1.1 Procédures d'exploitation documentées	Splunk permet aux entreprises de mettre en place une plateforme de données machine utilisant les mêmes procédures et outils pour tous les cas d'usage ou presque. Ce logiciel permet aux utilisateurs de poser différentes questions aux mêmes données pour les besoins d'équipes différentes. Cela permet aux équipes d'utiliser le même outil (et les mêmes données) pour les enquêtes de sécurité, la surveillance de sécurité, la validation de conformité, la détection des menaces, la supervision des services de bout en bout et encore d'autres cas d'usage du SIEM et des opérations IT.
12.1.2 Gestion des changements	Splunk peut être utilisé pour superviser les modifications apportées aux systèmes afin d'en consigner la date, l'auteur et le motif. C'est particulièrement utile pour comparer les situations d'urgence aux interruptions planifiées de certains systèmes. On peut évaluer les risques en fonction du nombre de modifications non autorisées et suivre ces chiffres afin de documenter la hausse ou la baisse du niveau de risque de l'entreprise. Il est également possible d'établir des corrélations avec les tickets de gestion des modifications.
12.1.3 Dimensionnement	Splunk peut superviser l'utilisation du CPU et d'autres informations de performances matérielles dans une infrastructure physique ou virtuelle. L'outil peut superviser les seuils au fil du temps et détecter les signes précurseurs d'une dégradation des performances. Les pannes matérielles partielles (touchant un ventilateur ou de la mémoire) peuvent être détectées et supervisées afin d'appuyer la planification des ressources et les décisions d'acquisition. Il est possible de superviser les services afin d'établir la performance des transactions à l'échelle de toute l'architecture IT. Ces données peuvent informer les investigations touchant l'architecture de livraison des services et enrichir les indicateurs de satisfaction des clients. Splunk permet d'établir des comparaisons avec les performances normales et de générer des alertes sur tous les aspects de la pile IP.
12.1.4 Séparation des environnements de développement, de test et d'exploitation	Splunk permet d'accéder aux logs des systèmes de production à des fins de dépannage sans qu'il soit nécessaire de se connecter à ces systèmes. C'est une exigence clé qui empêche les modifications non autorisées des systèmes.
12.2.1 Mesures contre les logiciels malveillants	Splunk facilite la collecte d'informations d'inventaire telles que les installations et les déploiements de paquets et d'applications. Ces informations peuvent être régulièrement actualisées et toute modification peut être signalée. Splunk permet aussi de rechercher les « menaces connues » et « inconnues ». Splunk supervise tous les aspects du déploiement d'antivirus, de la configuration des hôtes, de la sécurité de la messagerie, des produits de sécurité web et des pare-feu de nouvelle génération. Les menaces connues sont celles qu'ont signalées les systèmes basés sur des signatures et des règles. Splunk sait enrichir ces données à l'aide des données DNS et DHCP, les données d'accès physique, les données des logs Active Directory, et les données de capture et de flux de paquets. La recherche de combinaisons remarquables de données temporelles et géographiques peut permettre l'identification d'acteurs malveillants internes et de malwares persistants. On peut également renforcer l'alignement de la sécurité sur la stratégie commerciale en se concentrant sur les actifs les plus importants de l'entreprise.
12.2.1 Mesures contre les logiciels malveillants	Splunk facilite la détection des sites web frauduleux en examinant le trafic des pare-feu et des proxys, et en établissant des corrélations avec les URL fournies par les services tiers d'intelligence des menaces. Splunk peut aussi produire des rapports sur l'application des listes noires et les événements de prévention provenant des appliances de sécurité déployées.
12.2.1 Mesures contre les logiciels malveillants	Splunk permet d'accéder aux logs des systèmes à des fins de dépannage sans qu'il soit nécessaire de se connecter à ces systèmes. Splunk permet également de superviser les outils de protection contre les logiciels malveillants, produire des rapports et appuyer le processus de rétablissement grâce à des actions de réponse automatisées telles que la mise en quarantaine de l'hôte (déplacement vers un VLAN), le contrôle du nettoyage et la confirmation que l'hôte nettoyé ne présente plus aucun autre indicateur de compromission ni comportement réseau inhabituel.

Domaines clés d'ISO 27002	Appui fourni par Splunk et les données machine
12.2.1 Mesures contre les logiciels malveillants	Splunk délivre des informations constamment mises à jour sur les tactiques des menaces et propose de nouvelles techniques de détection et de réponse grâce à sa communauté et à son équipe de recherche en sécurité.
12.3.1 Sauvegarde des informations	Splunk supervise facilement les solutions de sauvegarde des données pour contrôler leur performance, l'intégrité des données et l'accès aux sauvegardes.
12.4.1 Journalisation des événements	Splunk peut superviser les systèmes de sécurité pour détecter les modifications de configuration lors des fenêtres de changement, et surveiller également le comportement des utilisateurs. Splunk fournit également un enregistrement définitif pour les audits de conformité.
12.4.1 Journalisation des événements	Splunk recueille tous les types de données de log ; si des informations manquent, Splunk peut enrichir les données grâce aux lookups de différentes sources. Splunk ajoutera automatiquement un horodatage et consignera l'hôte de provenance du log d'événements pour remédier à l'éventuelle absence de métadonnées.
12.4.1 Journalisation des événements	Splunk propose différents types et procédures d'anonymisation et de pseudonymisation, au niveau de la couche de présentation seulement ou jusqu'aux logs bruts conservés sur disque, selon les besoins de l'entreprise.
12.4.1 Journalisation des événements	Par défaut, Splunk est configuré pour empêcher toute suppression ou modification via l'interface utilisateur. On peut configurer des alertes pour signaler qu'une source de données a cessé d'envoyer ses logs ou que la configuration d'une politique de journalisation a été modifiée.
12.4.2 Protection de l'information journalisée	Le concept de rôle utilisateur chez Splunk, qui s'assortit d'une authentification robuste, assure que seuls les utilisateurs autorisés peuvent exploiter les données des logs d'événements. L'absence de modification peut être démontrée par une fonction d'Intégrité des données qui hache chaque portion de données brutes récemment indexée et l'inscrit dans un fichier "hash" qui peut lui aussi être sécurisé. Les suppressions d'événements de log seront documentées dans un journal d'audit interne et le comportement à adopter en cas d'épuisement de la capacité de stockage peut être configuré.
12.4.2 Protection de l'information journalisée	Splunk peut être configuré comme plateforme centrale pouvant transmettre les données à une autre solution Splunk ou agir comme système indépendant.
12.4.3 Journaux administrateurs et opérateurs	Splunk surveille toutes les activités des utilisateurs et en fournit un journal complet.
12.4.4 Synchronisation des horloges	Avec Splunk, vous pouvez superviser les systèmes pour assurer leur synchronisation grâce au protocole NTP. Splunk détectera également tout type de différence majeure dans l'horodatage des sources de données.
12.5.1 Installation de logiciels sur des systèmes en exploitation	Splunk peut superviser l'accès, la configuration et la performance des logiciels d'exploitation.
12.6.1 Gestion des vulnérabilités techniques	Splunk surveille la « demi-vie » des vulnérabilités des architectures IT et produit des rapports servant d'indicateurs pour les systèmes de correction. Les données des systèmes vulnérables peuvent être corrélées aux données d'attaque IDS/IPS pour identifier les tentatives d'exploitation des systèmes vulnérables.
12.6.1 Gestion des vulnérabilités techniques	Il est possible de générer des événements notables par système et par vulnérabilité puis de les suivre jusqu'à ce que le problème soit résolu, corrigé ou supprimé.

Domaines clés d'ISO 27002	Appui fourni par Splunk et les données machine
12.6.1 Gestion des vulnérabilités techniques	Splunk propose des tableaux de bord prêts à l'emploi pour documenter les opérations sur les vulnérabilités, qui consignent notamment les inspections et les hôtes qui n'ont pas encore été inspectés.
13.1.1 Contrôle des réseaux	Splunk prend en charge le contrôle des accès basé sur le rôle pour différentes équipes réseau. Splunk supervise les protocoles HTTP, HTTPS, SSL VPN et ceux de la couche d'application au niveau d'AppFlow ou d'un autre outil d'équilibrage des charges. Splunk peut aussi fournir des indicateurs portant sur l'aspect performance du matériel réseau, sur les modifications de configuration et sur la performance du réseau. Splunk utilise les données de log pour contrôler la fidélité des données en transit.
13.1.3 Cloisonnement des réseaux	Splunk surveille le trafic entre les réseaux et détecte le trafic non autorisé dans le cadre de la séparation des réseaux.
14.2.6 Environnement de développement sécurisé	Splunk supervise toutes les modifications apportées aux environnements de développement et au code qu'ils contiennent.
14.3.1 Protection des données de test	Splunk peut délivrer un suivi d'audit complet de l'accès aux données de test.
15.1.1 Politique de sécurité de l'information dans les relations avec les fournisseurs	Splunk supervise les canaux d'accès utilisés par les fournisseurs et documente toute l'activité qui s'y déroule.
15.1.2 La sécurité dans les accords conclus avec les fournisseurs	Splunk joue le rôle de plateforme centralisée sur laquelle on peut attribuer des accès à des tiers à des fins d'assistance et de collaboration. Splunk peut alors être utilisé par le fournisseur pour produire des rapports de conformité et démontrer l'efficacité des contrôles.
15.2.1 Surveillance et revue des services des fournisseurs	Si une entreprise a accès aux données de log de son prestataire de services, Splunk peut être employé pour contrôler les SLA. De plus, il est possible de superviser le cycle de vie des données hébergées par des tiers jusqu'à leur élimination. Le calcul des tendances des SLA appuie quant à lui les décisions d'acquisition de services.
16.1.1 Responsabilités et procédures	Splunk permet aux équipes de sécurité de répondre de façon rapide, efficace et structurée aux incidents et de faire le point sur leur portée et leur impact potentiel auprès de la direction. Les activités de gestion des incidents peuvent être consignées dans Splunk et placées sur une chronologie.
16.1.1 Responsabilités et procédures	Splunk soutient les équipes de réponse aux incidents en leur permettant de recueillir rapidement des données et de partager des informations sur les incidents avec des organismes externes si nécessaire.
16.1.2 Signalement des événements liés à la sécurité de l'information	Splunk Enterprise Security fournit des fonctions de gestion des événements de sécurité, d'alerte et de rapport.
16.1.4 Appréciation des événements liés à la sécurité de l'informations et prise de décision	Splunk fournit aux équipes une plateforme d'investigation des événements de sécurité qui leur permet d'évaluer s'ils doivent être classés comme incidents de sécurité des informations. Splunk aide les équipes de réponse aux incidents à prendre ces décisions.

Domaines clés d'ISO 27002	Appui fourni par Splunk et les données machine
16.1.5 Réponse aux incidents liés à la sécurité de l'information	Les fonctionnalités de Splunk ne se limitent pas à la détection et l'exploration des incidents : elles permettent aussi de documenter les actions de réponse sous la forme de procédures à exécuter ou à orchestrer automatiquement, et doublées d'un suivi d'audit à des fins d'analyse ultérieure.
16.1.5 Réponse aux incidents liés à la sécurité de l'information	Splunk permet aux utilisateurs d'explorer les historiques et des quantités massives de données machine provenant de centaines de technologies différentes afin d'identifier la source d'un incident dans le cadre d'une analyse post-mortem.
16.1.6 Tirer des enseignements des incidents liés à la sécurité de l'information	Splunk Enterprise Security offre un enregistrement complet de la classification des incidents et des changements de responsabilités.
16.1.7 Recueil de preuves	Splunk conserve les logs bruts générés par tous les types d'appareils et d'applications et peut effectuer un hachage des événements pour démontrer l'absence d'altération.
18.1.2 Droits de propriété intellectuelle	Splunk peut être utilisé pour produire des rapports sur les logiciels installés ou superviser l'utilisation des licences en l'absence de mécanismes techniques, pour avertir à l'avance des risques de violations. Splunk peut aussi identifier les licences inutilisées et les remettre dans la réserve de licences de l'entreprise.
18.1.3 Protection des enregistrements	Splunk protège les enregistrements à l'aide des concepts de mise en cluster et de haute disponibilité, la prise en charge des lecteurs WORM (supports non effaçables) et le hachage des fichiers.
18.1.3 Protection des enregistrements	Les enregistrements de Splunk sont compatibles avec différents systèmes de stockage, le hachage de fichier et la définition de politiques de conservation et de rotation des logs.
18.2.2 Conformité avec les politiques et les normes de sécurité	Splunk permet aux superviseurs d'élaborer des tableaux de bord dynamiques et de créer des rapports et des alertes pour automatiser et accélérer le processus d'examen régulier.
18.2.3 Examen de la conformité technique	Avec Splunk, une entreprise peut automatiser l'inspection de systèmes similaires en consignant les éléments à rechercher recommandés par une personne compétente et autorisée. Splunk peut aussi relever des mesures pertinentes et établir une supervision continue sur un même type d'applications, dans une optique de cohérence, de gain de temps et de sécurité.