splunk>

FICHE TECHNIQUE

Application Splunk® Enterprise Security

Une sécurité axée sur l'analyse comportementale et la détection de nouvelles menaces.

Faire face à des menaces en constante évolution

Une entreprise moderne a besoin de technologies de sécurité capables de s'adapter à un environnement de menaces dynamiques, aux tactiques d'adversaires qui évoluent et à des besoins d'entreprise en évolution constante. Pour faire face à ce nouveau contexte, les analystes sécurité doivent faire preuve d'agilité afin de réduire le délai de réaction et prendre des décisions pour limiter les risques pour l'entreprise. Pour répondre à ces nouveaux besoins, les équipes en charge de la sécurité doivent disposer de fonctionnalités d'analyse avancées et du contexte associé aux incidents pour identifier rapidement les nouvelles techniques d'attaque.

Cet environnement de menaces en évolution permanente se distingue notamment par le fait que les agresseurs possèdent le temps, l'expertise et les ressources nécessaires pour mettre au point des scénarios capables de contourner les fonctions de détection des produits de sécurité et les systèmes traditionnels de corrélation des événements de sécurité (SIEM). Leurs actions sont dissimulées par les téraoctets de données générées par les activités normales des utilisateurs. Ces pirates tenaces ont compris que de nombreuses équipes de sécurité ne peuvent pas voir ces attaques, du fait de leur cloisonnement par silos, de difficultés de collecte, de problèmes liés au volume des données ou du manque de capacités analytiques. Les équipes de sécurité peuvent contrer ces attaquants en enrichissant toutes les données utiles pour la sécurité avec des informations de contexte afin d'analyser les activités suspectes. Lorsque l'analyse est enrichie de flux de renseignements sur les menaces, les analystes peuvent identifier les menaces précédemment inconnues pour y réagir de manière proactive. D'autres sources de données d'entreprise peuvent ajouter un contexte supplémentaire (ex. systèmes de gestion des horaires, bases de données RH, bases de données d'actifs) afin de détecter et comprendre les menaces internes, et en particulier les fraudes et les vols de propriété intellectuelle. Face à l'évolution constante des menaces, les équipes chargées de la sécurité doivent recourir à des outils basés sur l'analyse pour faire coïncider la posture de sécurité et les risques commerciaux.

Pour détecter les menaces sophistiquées et repousser les intrus, il faut adopter une approche basée sur les risques qui ne peut être mise en place qu'à l'aide d'une plate-forme orientée big data, capable d'exploiter des volumes de données importants. Cette plate-forme doit ingérer toutes les données machine et les diverses sources de renseignements sur les menaces pour pouvoir les mettre en corrélation avec les informations choisies par l'analyste. Ces capacités permettent à l'analyste sécurité de faire preuve de créativité, d'exploiter des visualisations et d'utiliser de l'analyse statistique pour faciliter l'identification des menaces inconnues.

Définition de la sécurité axée sur l'analyse :

Processus consistant à découvrir des relations entre toutes les données utiles pour la sécurité, notamment les données provenant des infrastructures informatiques, des produits de sécurité et toutes les données générées par les machines, afin de s'adapter rapidement à un environnement de menaces en constante évolution.

L'application Splunk Enterprise Security

Déployée pour la surveillance permanente, la prise en charge des incidents, dans un centre d'opérations de sécurité ou à destination des décideurs qui veulent avoir une visibilité sur les risques métier, l'Application Splunk Enterprise Security (ES) offre la flexibilité nécessaire pour élaborer des vues personnalisées selon des besoins spécifiques. L'Application Splunk Enterprise Security comprend notamment une fonction de capture de flux réseaux activable d'un simple click, un framework d'intelligence opérationnelle simple d'utilisation, des règles de corrélation, ainsi que de détection de seuils évoluant automatiquement. Ces fonctionnalités combinées vous permettent de surveiller les menaces connues et inconnues. L'application ES comprend les fonctionnalités suivantes :

Analyse et classification des incidents : dans le cadre d'une fonction complète d'analyse des incidents, la classification permet d'appliquer des réaffectations, des changements d'état et des classifications de sévérité à des groupes d'événements, tout en permettant d'auditer l'ensemble de l'activité des analystes.

Rapports et indicateurs de sécurité : exploitez des dizaines de rapports, tableaux de bord et indicateurs prédéfinis ; un graphique, un tableau de bord ou un tableau peut être créé à partir de n'importe quel résultat de recherche afin de transformer des données brutes et non-structurées en données d'analyse ; exportez les données d'origine au format PDF ou CSV.

Analyse basée sur les risques : alignez votre position en matière de sécurité sur les besoins de l'entreprise en appliquant un risque à tout type de données et en révélant en toute transparence les facteurs qui contribuent à ce risque ; affectez rapidement et facilement un KSI/KPI à un événement pour produire un indicateur de risque à l'aide du framework de risques.

Framework d'analyse des menaces : intègre, dé-duplique et attribue des priorités à toute source d'intelligence publique, propriétaire ou locale, et en fait un composant essentiel de vos opérations de sécurité.

Éditeur de recherche unifié : une expérience de recherche conviviale et cohérente, incluant un assistant de création de règles, pour les recherches de corrélation d'indicateurs clés de sécurité (KSI) ou d'indicateurs clés de performance (KPI) et pour visualiser les recherches d'identités et d'actifs (voir Figure 1)

Figure 1. Enterprise Security 3.2 : Tableau de bord de position de sécurité

Analyse statistique : des tableaux de bord prédéfinis permettent d'identifier les anomalies présentes dans les données d'événements et de protocoles à l'aide de seuils et de références configurées automatiquement

Tableaux de bord personnalisables : créez votre propre portail de sécurité selon votre rôle dans ce que l'entreprise considère comme important (voir Figure 2) ; organisez et corrélez visuellement différentes sources de données au sein d'une même interface afin d'identifier des relations et d'obtenir des informations contextuelles

Grâce à la collecte de toutes les données indexée de manière chronologique, l'absence de normalisation au préalable et la possibilité d'appliquer un schéma de données au moment de la recherche, la plate-forme élimine tous les obstacles à la collecte et à la visualisation des données applicatives et opérationnelles permettant de donner du contexte aux incidents de sécurité. La plate-forme Splunk peut collecter tout type de données – structurées ou non – des systèmes d'information, de sécurité et industriel, et de toute autre source de données machine, puis afficher ces données pour les opérations de sécurité, avec le contexte issu de la gestion du changement et de l'accès physique. Splunk Enterprise et l'application Splunk Enterprise Security offrent une solution de supervision de sécurité à la fois unique, flexible et évolutive qui va bien au-delà des limites des technologies de SIEM traditionnelles.

Présentation générale de l'Application Splunk Enterprise Security

Indicateurs de sécurité

Bénéficiez d'une bibliothèque de widgets d'indicateurs de sécurité, à intégrer à n'importe quel tableau de bord, ou créez facilement le vôtre. Observez les événements de sécurité par emplacement, hôte, type de source, groupes d'actifs et localisation géographique. Les KPI fournissent en temps réel des informations de tendance sur votre niveau de sécurité et en assurent la surveillance.

Examen des incidents et investigations

L'Application Splunk Enterprise Security permet d'explorer les données d'origine en cliquant depuis l'interface graphique et de capturer les flux réseaux afin de comprendre tous les échanges réseau. Les opérations uniques du workflow renforcent le processus d'investigation de sécurité et permettent à l'utilisateur de travailler à partir d'une seule information commune ou de toute autre donnée pour analyser rapidement le contexte de la menace.

Protection des accès

Simplifiez la surveillance du contrôle d'accès, l'analyse des exceptions et les processus d'audit des applications, des systèmes d'exploitation et des systèmes de gestion des identités à l'échelle de toute l'entreprise. Respectez les exigences de conformité et d'investigation en surveillant les utilisateurs privilégiés et les tentatives d'accès système à toutes les applications stratégiques de l'entreprise.

Protection des terminaux

Renforcez l'efficacité des produits de sécurité tels que Symantec™ Endpoint Protection, IBM® Proventia Desktop ou McAfee® Endpoint Protection. Hiérarchisez les menaces et observez les tendances à long terme. La protection des terminaux comprend des recherches, des rapports et une liste d'alertes au sujet des logiciels malveillants, des activités inhabituelles ainsi que de la consommation et la disponibilité des ressources.

Protection du réseau

Surveillez et détectez les événements des équipements réseau et sécurité à l'échelle de l'entreprise. Découvrez les anomalies protocolaires, les pare-feu, les routeurs, les serveurs DHCP, les points d'accès sans fil, les load-balancers, les IDS et les dispositifs de DLP. Exploitez des corrélations, des recherches, des rapports et des tableaux de bord pour superviser l'activité réseau et générer des alertes.

Centre des assets / Centre des identités

Comprendre où se trouvent les actifs, qui les possède, quelle est leur criticité et qui doit pouvoir accéder aux informations stratégiques des systèmes permet de hiérarchiser les événements de sécurité et les investigations. L'application exploite la capacité de Splunk à effectuer des recherches en temps réel sur les données stockées dans des bases d'assets, Active Directory, des tableurs et des fichiers CSV, pour ensuite utiliser ces informations afin d'ajouter du contexte aux événements de sécurité dans des rapports et des tableaux de bord.

Analyse des risques

Identifiez les sources de risque dans votre environnement, leur amplitude et les facteurs favorisant le comportement à risque. Utilisez des indicateurs de risque pour découvrir les activités inhabituelles.

Audit des incidents

À des fins de gouvernance, d'audit et de protection contre les altérations, l'Application Splunk Enterprise Security fournit des rapports sur toutes les activités des utilisateurs de Splunk et des systèmes afin de fournir un audit complet. La plate-forme Splunk utilise des mécanismes de signatures pour préserver la chaîne de responsabilité et détecter les éventuelles modifications dans les log et les événements d'origine.

Figure 2. Enterprise Security 3.2 : Inspecteur d'actifs

Téléchargement gratuit

Téléchargez Splunk gratuitement. Vous recevrez une licence Splunk Enterprise 6 valable pendant 60 jours et pourrez indexer jusqu'à 500 Mo de données par jour. Au bout de 60 jours ou à tout moment avant l'expiration du délai, vous pouvez passer à une licence Gratuite perpétuelle ou acheter une licence Entreprise en contactant emea_sales@splunk.com.

Splunk Inc., 5 place de la Pyramide, Tour Ariane La Défense 9, La Défense Cedex, 92088 Paris info@splunk.com | emea_sales@splunk.com
+33 1 55 68 10 43 apps.splunk.com

Item # FS-SPLUNK-AppEntSec-117-A4