LIVRE BLANC

Les sept fonctionnalités essentielles d'un SIEM orienté analyse

Les menaces modernes exigent une sécurité axée sur l'analyse et une supervision continue

splunk> turn data into doing™

Les SIEM traditionnels appartiennent au passé

Il est relativement facile de trouver un mécanisme pour recueillir, stocker et analyser les données si l'on se limite à la sécurité. Les options de stockage des données sont nombreuses. En revanche, compiler toutes les données utiles pour la sécurité et les transformer en renseignements exploitables est une toute autre mission.

Bien des départements IT d'entreprises ont fait la pénible expérience de cette dure vérité après avoir investi dans une plateforme SIEM (gestion des informations des événements de sécurité). Après avoir consacré beaucoup de temps et d'argent à l'enregistrement des événements de sécurité, il apparaît que l'assimilation de ces données a pris un temps considérable, et surtout que le système de données sous-jacent utilisé pour créer le SIEM tend à être statique.

Pire encore, les données disponibles pour analyse ne sont fondées que sur les événements de sécurité. Il devient donc difficile de corréler les événements de sécurité avec le reste de l'activité de l'environnement IT. En cas de problème, l'exploration d'un événement de sécurité exige un temps précieux, ce que ne peuvent se permettre la plupart des organisations.

De plus, le système SIEM ne parvient pas à tenir le rythme imposé par l'urgence de l'exploration des événements de sécurité. La poursuite de l'adoption des services cloud élargit les vecteurs de menaces et les entreprises doivent désormais superviser l'activité des utilisateurs, les comportements et l'accès aux applications sur les services cloud, SaaS, mais aussi locaux, afin de déterminer toute l'envergure des menaces et attaques potentielles.

Aujourd'hui, l'informatique d'entreprise a besoin d'un moyen simple de corréler l'ensemble des données qui lui permettent de gérer sa position de sécurité. Au lieu de se contenter d'examiner les événements après qu'ils se sont produits, le service IT doit anticiper leur apparition et mettre en place des mesures pour limiter les vulnérabilités en temps réel. Et pour cela, les entreprises ont besoin d'une plateforme SIEM axée sur l'analyse.

Un SIEM axé sur l'analyse permet à l'IT de superviser les menaces en temps réel et de réagir rapidement aux incidents, afin que les dommages puissent être évités ou limités. Mais les attaques ne proviennent pas toutes de l'extérieur, et l'IT doit pouvoir superviser l'activité de ses utilisateurs pour minimiser les risques de menaces internes ou de compromission accidentelle. L'intelligence des menaces est cruciale

Fonctionnalités essentielles d'un SIEM orienté analyse	
Supervision en temps réel	Les menaces évoluent rapidement et l'IT doit pouvoir les superviser et corréler les événements en temps réel pour localiser et arrêter les menaces au plus tôt.
Réponse aux incidents	L'IT doit disposer d'une approche structurée pour prendre en charge et gérer les failles potentielles ainsi que les conséquences d'un incident ou d'une attaque, afin de limiter les dommages et de réduire les coûts et le délai de rétablissement.
Supervision des utilisateurs	Il est indispensable de superviser l'activité des utilisateurs en contexte pour localiser les failles avec précision et mettre au jour les usages illégaux. La supervision des utilisateurs privilégiés est une exigence courante dans les rapports de conformité.
Intelligence des menaces	L'intelligence des menaces aide l'IT à identifier les activités anormales, à évaluer les risques pour l'entreprise et hiérarchiser la réponse.
Analyses avancées	L'analyse est la clé qui permet d'extraire des renseignements à partir de montagnes de données, et le machine learning peut automatiser cette analyse pour identifier les menaces invisibles.
Détection des menaces avancées	Les professionnels de sécurité ont besoin d'outils spécialisés pour superviser, analyser et détecter les menaces sur toute la kill-chain.
Bibliothèque de cas d'usage	Colonne de droite : Les entreprises doivent impérativement comprendre et prendre en charge les menaces en temps réel pour réduire leur niveau de risque.

pour comprendre la nature de l'environnement de menaces au sens large, et pour replacer ces menaces en contexte. Un SIEM axé sur l'analyse doit naturellement exceller dans le domaine de l'analyse de sécurité, et mettre à la disposition des équipes IT des méthodes quantitatives sophistiquées et puissantes pour obtenir des renseignements et hiérarchiser
leurs efforts. Enfin, un SIEM moderne doit intégrer, au sein de sa plateforme de base, les outils spécialisés nécessaires pour lutter contre les menaces avancées.

Un SIEM orienté analyse doit rassembler sept fonctionnalités essentielles :

Ces capacités leur permettent d'exploiter leur SIEM dans une large gamme de cas d'usage de sécurité et de conformité. Examinons de plus près chaque fonction essentielle d'un SIEM axé sur l'analyse.

Supervision en temps réel

Plus il faut de temps pour découvrir une menace, et plus elle peut infliger de dommages. Les organisations IT doivent être armées d'un SIEM offrant des fonctions de supervision pouvant s'appliquer en temps réel à n'importe quel jeu de données, qu'il soit stocké localement ou dans le cloud. De plus, cette fonction de supervision doit pouvoir extraire à la fois les flux de données contextuels tels que les données d'actifs et d'identité, mais aussi les flux d'intelligence des menaces, qui permettent de produire des alertes.

Un SIEM axé sur l'analyse doit être capable d'identifier toutes les entités de l'environnement IT – utilisateurs, machines et applications – et toute activité qui n'est pas spécifiquement rattachée à une identité. Le SIEM doit pouvoir utiliser ces données en temps réel pour identifier un large éventail de types et de classes de comportements anormaux. Une fois cela fait, il faut pouvoir injecter facilement les données dans un workflow créé pour évaluer les risques qu'une anomalie peut présenter pour l'entreprise.

Le SIEM doit être accompagné d'une bibliothèque de règles de corrélation personnalisables et prédéfinies, une console d'événements de sécurité qui présente en temps réel les incidents et les événements de sécurité, et des tableaux de bord montrant des visualisations en temps réel des activités menaçantes.

Enfin, toutes ces compétences doivent s'enrichir de recherches de corrélation prêtes à l'emploi pouvant être invoquées en temps réel ou selon un planning défini. Tout aussi utile, ces recherches doivent être accessibles à l'aide d'une interface intuitive évitant d'avoir recours à un administrateur IT ou de maîtriser un langage de recherche.

N'oublions pas non plus qu'un SIEM axé sur l'analyse doit permettre de faire des recherches localement dans les données temps réel et historiques, de façon à réduire le trafic réseau lié à l'accès aux données stockées sur site, dans le cloud ou les deux.

Réponse aux incidents

Au cœur d'une stratégie efficace de réponse aux incidents se trouve une plateforme SIEM robuste qui permet non seulement d'identifier les différents incidents, mais offre également les moyens de les suivre, de les affecter et de les annoter.

L'IT doit fournir aux autres membres de l'entreprise des niveaux d'accès variables en fonction de leur rôle. Une organisation IT souhaitera aussi agréger des événements de façon manuelle ou automatique, bénéficier d'interfaces de programmation (API) utilisables pour échanger des données avec des systèmes tiers, collecter des données probantes légalement valables et mettre en place des procédures pour guider les équipes pas-à-pas dans la prise en charge d'incidents spécifiques.

Surtout, un SIEM axé sur l'analyse doit inclure des capacités de réponse automatique pouvant interrompre les cyberattaques en cours.

En effet, la plateforme SIEM doit être le centre autour duquel s'articulera un workflow personnalisable de gestion des incidents. Bien sûr, les incidents ne présentent pas tous le même degré d'urgence. Une plateforme SIEM axée sur l'analyse fournit aux départements IT les moyens de catégoriser la gravité d'une menace potentielle. Grâce à des tableaux de bord utilisables pour trier les nouveaux événements notables, les affecter à des analystes et examiner les informations associées pour produire des pistes d'investigation, un SIEM axé sur l'analyse arme les départements IT des renseignements contextuels nécessaires pour déterminer la réponse appropriée à tout type d'événement.

On doit aussi pouvoir identifier les événements notables et leur état, indiquer la gravité des événements notables, lancer un processus de correction et fournir un audit de l'intégralité du processus entourant l'incident.

Enfin, l'équipe IT doit disposer d'un tableau de bord permettant d'appliquer intuitivement des filtres à n'importe quel champ au cours d'une investigation afin d'élargir ou réduire la portée de l'analyse en quelques clics. L'objectif final doit toujours être de permettre à n'importe quel membre de l'équipe de sécurité de placer des événements, des actions et des annotations sur une chronologie grâce à laquelle les autres membres de l'équipe pourront facilement comprendre la situation. Ces chronologies peuvent ensuite être incluses dans un journal donnant ensuite la possibilité d'étudier l'attaque et de mettre en place une méthodologie de kill-chain reproductible, pour prendre en charge les événements de ces types particuliers.

Supervision des utilisateurs

Au strict minimum, la supervision de l'activité des utilisateurs doit offrir la possibilité d'analyser les données d'accès et d'authentification, établir le contexte de l'utilisateur et produire des alertes en cas de comportement suspect et d'infraction aux politiques de l'entreprise et aux directives réglementaires.

Il est absolument essentiel que la supervision des utilisateurs soit étendue aux utilisateurs privilégiés qui sont les plus souvent visés par les attaques et peuvent causer le plus de dommages en cas d'usurpation. En effet, en raison de ce risque, la supervision des utilisateurs privilégiés est une exigence courante dans les rapports de conformité.

Pour atteindre ces objectifs, il faut des vues en temps réel et des capacités de rapports exploitant divers mécanismes d'identités capables de couvrir un nombre illimité d'applications et de services tiers.

Intelligence des menaces

Un SIEM axé sur l'analyse doit proposer deux formes différentes d'intelligence des menaces. La première repose sur l'utilisation de services d'intelligence des menaces qui fournissent des informations actualisées sur les indicateurs de compromission, les tactiques, techniques et procédures adverses, ainsi que du contexte supplémentaire sur différents types d'incidents et d'activité. Ces renseignements facilitent la reconnaissance des activités anormales comme, entre autres, l'identification de connexions sortantes vers une adresse IP externe connue pour être un serveur de commande et contrôle actif. Avec ce niveau d'intelligence des menaces, les analystes détiennent les informations nécessaires pour évaluer les risques, l'impact et les objectifs d'une agression – des aspects cruciaux pour hiérarchiser et adapter la réponse.

La deuxième forme d'intelligence consiste à évaluer le caractère critique d'un actif, son utilisation, sa connectivité, ses propriétaires et, en dernier lieu, le rôle, la responsabilité et le statut d'emploi de l'utilisateur.

Ce contexte supplémentaire est souvent crucial quand il s'agit d'évaluer et analyser le risque et l'impact potentiel d'un incident. Par exemple, un SIEM axé sur l'analyse doit pouvoir incorporer les informations de lecture de badge des employés et corréler ces données avec les logs d'authentification du VPN pour produire du contexte sur l'emplacement d'un employé dans le réseau de l'entreprise. Pour délivrer des niveaux d'analyse et d'intelligence opérationnelle plus profonds encore, le SIEM doit aussi utiliser les API REST pour récupérer, via une action de workflow ou un script, ces informations de contexte et les injecter dans le système, ainsi que pour combiner des données structurées issues de bases de données relationnelles avec des données machine.

Les données d'intelligence des menaces doivent idéalement être intégrées avec les données machine générées par divers types d'infrastructures IT et d'application pour créer des listes de supervision, des règles de corrélation et des requêtes, afin d'accroître le taux de réussite de la détection précoce des failles. Ces informations doivent être automatiquement corrélées aux données d'événements et ajoutées aux vues et rapports des tableaux de bord, ou bien transmises à des pare-feux ou autres systèmes de prévention des intrusions capables de résoudre la vulnérabilité en question.

Le tableau de bord fourni par le SIEM doit suivre l'état et l'activité des produits de détection des vulnérabilités déployés dans l'environnement IT, réaliser des contrôles de santé des systèmes de balayage et identifier les systèmes qui ne sont plus supervisés.

Pour résumer, une couche complète d'intelligence des menaces doit prendre en charge n'importe quelle liste de menaces, identifier automatiquement les renseignements redondants, identifier et hiérarchiser

les menaces figurant dans plusieurs listes et attribuer une pondération aux différentes menaces afin d'évaluer le risque réel qu'elles représentent pour l'entreprise.

Analyses avancées

L'analyse avancée emploie des méthodes quantitatives sophistiquées telles que les statistiques, l'exploration de données descriptive et prédictive, la simulation et l'optimisation pour produire de nouveaux renseignements cruciaux. Les méthodes d'analyse avancée incluent la détection des anomalies, le profilage des groupes de paris et la modélisation des relations des entités.

Tout aussi important, un SIEM axé sur l'analyse doit comprendre des outils permettant de visualiser et corréler les données, par exemple en cartographiant des événements catégorisés sur une kill-chain ou en créant des cartes de chaleur pour mieux appuyer les investigations.

Pour rendre tout cela possible, il faut accéder à une plateforme SIEM employant des algorithmes de machine learning capables d'apprendre par eux-mêmes ce qui distingue un comportement normal d'une véritable anomalie.

Ce niveau d'analyse des comportements doit ensuite être utilisé pour élaborer, valider et déployer des modèles prédictifs. Il doit même être possible d'exploiter des modèles créés à partir d'outils tiers.

Détection des menaces avancées

Les menaces de sécurité évoluent constamment. Un SIEM axé sur l'analyse s'adapte aux nouvelles menaces avancées grâce à la mise en œuvre de la supervision de la sécurité du réseau, la détection des points de terminaison, l'isolement des problèmes et l'analyse des comportements, en combinaison les uns avec les autres, pour identifier les nouvelles menaces potentielles et les mettre en quarantaine. La plupart des pare-feux et des systèmes de protection contre les intrusions ne suffisent pas à remplir ces fonctions.

L'objectif n'est pas seulement de détecter les menaces, mais aussi d'en déterminer la portée en localisant la destination possible d'une menace avancée après sa détection initiale, en déterminant comment la contenir et en choisissant les informations à partager.

Au final, un SIEM axé sur l'analyse doit pouvoir corréler différents mécanismes de défense contre les menaces persistantes avancées.

Bibliothèque de cas d'usage

Non seulement les événements de sécurité évoluent constamment, mais les analystes doivent aussi détecter et prendre en charge les menaces à vitesse réelle. Une solution SIEM axée sur l'analyse renforce la position de sécurité d'une entreprise en proposant du contenu prêt à l'emploi et pertinent. Une bibliothèque de cas d'usage peut également aider les analystes à découvrir automatiquement de nouveaux scénarios d'utilisation et identifier ceux qui s'appliquent à leur environnement en fonction des données assimilées. Cela permet, à terme, de réduire les risques en accélération la détection et la prise en charge des menaces continues ou récemment découvertes.

Un SIEM capable de produire de l'intelligence exploitable

Les SIEM portent de nombreuses promesses mais les systèmes traditionnels ne sont pas à la hauteur du rythme et de la sophistication des cyberattaques d'aujourd'hui.

Les entreprises d'aujourd'hui doivent s'équiper de SIEM axés sur l'analyse combinant une plateforme big data optimisée pour les données machine avec des fonctions d'analyse avancée et de détection des menaces, des outils de supervision et de réponse aux incidents, ainsi que différentes formes d'intelligence des menaces. Sans ces compétences stratégiques, l'IT souffrira toujours d'un handicap fondamental lorsqu'il faudra défendre l'environnement IT contre les cybercriminels qui travaillent pour de grandes organisations et états-nations et jouissent de ressources quasi-illimitées.

L'un des meilleurs moyens de combattre ces menaces consiste à exploiter un SIEM axé sur l'analyse, capable de combiner des données opérationnelles IT et de l'intelligence de sécurité de manière à identifier en temps réel les vulnérabilités spécifiques visées par ces organisations. Armées de ces données, les équipes de sécurité informatique peuvent remédier aux menaces connues et anticiper les nouvelles, en temps réel, afin de minimiser les dommages potentiels pour l'entreprise. On est bien loin des

anciens SIEM qui collectaient les événements de sécurité sans pouvoir en faire des renseignements véritablement exploitables.

Le fait est que la plupart des organisations IT sont désormais évaluées sur leur capacité à repousser ces attaques, mais on peut difficilement empêcher les cybercriminels de les lancer. Pire encore, la plupart des départements IT ne disposent pas des ressources humaines requises pour faire face seuls à ces attaques. C'est la robustesse de la plateforme SIEM d'une entreprise qui fera d'une attaque un simple désagrément de routine ou un événement catastrophique.

La bonne nouvelle, c'est qu'il n'a jamais été aussi simple de mettre un SIEM en place. Si l'on ajoute à cela que la sophistication d'un SIEM moderne peut maintenant s'appliquer à défendre l'environnement informatique, alors la question n'est plus de savoir si une entreprise a besoin d'un SIEM, mais à quelle vitesse elle peut en installer un avant la prochaine vague de cyberattaques.

Voulez-vous savoir quelles sont les capacités essentielles d'un SIEM orienté analyse ? **Découvrez quelles sont les fonctionnalités stratégiques du SIEM selon Gartner et pourquoi l'agence a désigné Splunk comme leader dans le domaine** pour la septième fois.

splunk>

En savoir plus : www.splunk.com/asksales

www.splunk.com

2020-SPLK-SEC-Seven Essential Capabilities SIEM-FR-102-A4-WP