Guide essentiel

Analyse du comportement des utilisateurs et des entités

Détectez les menaces avancées grâce au machine learning, obtenez des informations riches et contextualisées pour comprendre les attaques et harmonisez le travail d'investigation des incidents.

splunk>

Les équipes de sécurité sont confrontées à des défis plus nombreux que jamais : la surface d'attaque s'élargit, les vulnérabilités se multiplient et les cyberattaques sont maintenant incessantes. Et tous ces facteurs augmentent considérablement le risque organisationnel. Selon le rapport de Splunk État de la cybersécurité en 2023, les centres d'opérations de sécurité (SOC) sont tellement débordés que 23 % des analystes SOC déclarent avoir du mal à gérer les volumes d'alertes de sécurité. Il y en a tellement à traiter que 41 % d'entre elles sont ignorées. Les menaces parviennent ainsi à traverser les défenses d'une organisation. Le temps moyen de détection (MTTD) augmente et le temps de séjour des menaces se prolonge. En effet, les organisations évoquent un temps de séjour moyen de 2,24 mois, et 52 % des organisations ont signalé des violations au cours des deux dernières années.

Ces défis sont exacerbés par l'accélérateur que constitue l'IA générative. Selon le rapport Prévisions 2024 pour la sécurité de Splunk, les pirates vont créer des logiciels malveillants évasifs conçus par l'IA, des contrefaçons sophistiquées (les « deepfakes ») et des tactiques d'ingénierie sociale toujours plus performantes. Nous devrions également voir émerger de nouveaux types d'attaques en 2024 : des campagnes de désinformation commerciale et économique, notamment, avec des attaques plus ciblées contre les marques et la réputation des entreprises. Les auteurs de ransomwares s'appuieront de plus en plus sur des menaces zero-day pour infiltrer les réseaux.

Des cyberattaques d'un tel niveau de sophistication peuvent être très difficiles à découvrir et à détecter. Même si les règles de corrélation créées par l'homme peuvent détecter les comportements malveillants, il serait illusoire de penser qu'elles identifient 100 % des menaces présentes dans un environnement. Gardez en tête les limites des tactiques de sécurité reposant uniquement sur l'humain. Les équipes de sécurité sont tellement submergées par le volume et la sophistication des attaques qu'elles ont atteint les limites de leur capacité à observer, s'orienter, décider et agir efficacement et rapidement. Une stratégie plus judicieuse consisterait à allier l'humain à la machine, pour décupler les capacités de l'équipe SOC en lui donnant une technologie capable de rationaliser et d'automatiser les aspects clés du cycle de détection, d'investigation, de réponse et de correction.

C'est là que le machine learning (ML) change la dynamique. Le machine learning n'émet aucune hypothèse de départ. Il n'a pas d'idée préconçue de ce qui est bon ou mauvais. Au lieu de cela, il s'entraîne : il apprend ce qui est normal et ce qui constitue une anomalie. Sans aucun biais inhérent, il apprend de l'environnement pour établir une base de référence, et tout ce qui se comporte de manière atypique ou qui se départit de cette base est considéré comme anormal.

Qu’est-ce que l’analyse du comportement des entités et des utilisateurs ?

L’analyse du comportement des entités et des utilisateurs (UEBA) s’intéresse au comportement des personnes, des appareils (routeurs, serveurs, etc.) et des applications. Elle utilise le machine learning pour détecter les comportements inhabituels. Une solution de ce type supervise les comptes utilisateurs, les appareils et les applications présents dans l’environnement, analyse leurs habitudes d’accès et émet des alertes en cas de signe de comportement anormal. Quelques exemples de comportements potentiellement anormaux :

- Quelqu’un se connecte à un compte utilisateur à partir d’un appareil, d’un navigateur ou d’un emplacement géographique inhabituel. On observe plusieurs tentatives de connexion infructueuses à un compte utilisateur pour lequel aucun échec de connexion n’a été enregistré jusque-là.
- Un utilisateur qui n’est pas autorisé à accéder à des fichiers, des répertoires ou d’autres ressources à partir d’un compte privilégié tente d’y accéder, ce qui peut indiquer un abus de compte privilégié.
- Un utilisateur télécharge des fichiers volumineux alors que ce n’est pas dans ses habitudes de le faire.
- Un utilisateur commence soudainement à transférer de grandes quantités de données, ce qui peut indiquer qu’il exfiltre des informations sensibles du système.
- Un utilisateur exécute des commandes inhabituelles ou des scripts qu’il n’utilise jamais ou qui ne correspondent pas à son rôle professionnel. Par exemple, un membre du service marketing exécute une requête de base de données complexe.
- Une application reçoit soudainement des milliers de requêtes de plus que d’habitude en dehors des heures de pointe traditionnelles. Ce type de comportement peut être le signe d’une attaque DDoS.

Comment un système UEBA identifie-t-il ce type d’anomalies ? Malgré toute leur diversité, les cyberattaques ont un point commun : le comportement d’un utilisateur ou d’un actif compromis dévie de ses habitudes ou de celles de son groupe de pairs. Ce changement de comportement fournit des indicateurs de compromission (IoC) qui peuvent être reliés les uns aux autres pour mettre une menace en évidence.

Le comportement des entités – en particulier des utilisateurs, dispositifs, comptes système et comptes privilégiés – peut être analysé pour révéler des anomalies, même lorsqu’elles se produisent rarement et sur des périodes étendues. Une solution UEBA peut relever l’empreinte de ces acteurs malveillants lorsqu’ils traversent les environnements d’entreprise, cloud et mobiles, puis les analyser à l’aide d’algorithmes avancés de machine learning pour établir une base de référence, détecter les écarts et signaler les anomalies en continu.

Ces aberrations sont ensuite assemblées sous forme de séquences logiques grâce à la détection de modèles et à une corrélation avancée pour mettre au jour les véritables « kill-chains » parfaitement intelligibles et immédiatement exploitables. La kill-chain décrit la réalité d’une attaque, c’est-à-dire une séquence d’activités malveillantes qui aboutissent à une violation. À chaque étape de la séquence, il arrive souvent que plusieurs événements révèlent le parcours et le comportement d’un attaquant. Contrairement aux alertes qui se déclenchent lorsqu’un seuil défini est franchi, la détection des menaces basée sur le comportement utilise le machine learning et une connaissance très pointue du contexte pour maximiser la probabilité de trouver des menaces réelles et invisibles tout en minimisant le taux de faux positifs.

Les cinq fonctionnalités essentielles de l'analyse du comportement des utilisateurs et des entités

Voici les cinq fonctionnalités que toute solution d'analyse du comportement des utilisateurs et des entités de pointe devrait posséder :

1. Couverture des utilisateurs, entités, appareils et applications

Les premiers produits d'analyse comportementale examinaient simplement les comportements des utilisateurs. Lorsque vous comparerez des solutions UEBA, assurez-vous que la technologie analyse et supervise aussi bien les utilisateurs que les entités. Elle doit couvrir le comportement des utilisateurs finaux, des terminaux, des serveurs, des routeurs, des applications, etc. Examinez attentivement les domaines couverts par les solutions UEBA que vous envisagez pour garantir une supervision complète de tous les aspects de votre entreprise.

Pensez également qu'une solution UEBA de pointe doit analyser les données provenant de plusieurs sources, notamment les :

- bases de données comme Active Directory,
- outils de sécurité : antivirus, EDR et EPP (détection des terminaux et réponse ou plateforme de protection des terminaux), systèmes de prévention des intrusions (IPS/NGIPS) et SIEM, naturellement,
- outils de sécurité réseau : routeurs, pare-feu, accès des identités et VPN,
- flux de threat intelligence.

2. Capacités de détection et d'analyse alimentées par le machine learning

Une solution UEBA de pointe ne peut pas se contenter de règles de corrélation pour ses recherches et ses détections. Si les règles de corrélation rédigées par des humains parviennent effectivement à repérer certains comportements malveillants, elles ne suffisent pas à identifier 100 % des menaces dans un environnement. Mais le machine learning peut combler cette lacune. Les solutions UEBA de premier plan l'utilisent pour détecter les menaces invisibles et inconnues ainsi que les comportements anormaux des utilisateurs, des terminaux et des applications.

De quelle façon ? La solution UEBA crée des bases de référence et établit les plages « normales » de comportement et d'activité de chaque utilisateur et entité. Cette base de référence comporte plusieurs dimensions configurables et elle peut être comparée aux bases de référence d'un service, d'une région ou d'une entreprise. Les organisations peuvent ainsi identifier et suivre un utilisateur qui, alors qu'il n'imprime habituellement que quelques pages à la fois, se met soudainement à en imprimer une cinquantaine. Cet événement sera considéré comme un comportement anormal pour cet utilisateur précis. En revanche, l'utilisateur qui imprime régulièrement 200 pages par jour ne fera l'objet d'aucun signalement, à moins qu'il ne dépasse considérablement sa base de référence. Ces alertes personnalisées sont très puissantes car elles permettent de cibler précisément des menaces connues. Rapides à rédiger, ces conditions permettent de détecter des événements futurs et sont suffisamment simples pour que les analystes de sécurité puissent les interpréter et agir.

Le machine learning prend en charge des scénarios d'utilisation avancés qui ne doivent pas être gérés uniquement par des approches conventionnelles. Les solutions UEBA utilisent le ML pour accroître la portée et l'échelle de méthodes de détection simples (généralement basées sur des signatures ou sur des règles de corrélation) afin d'améliorer globalement les performances. Si les seuils et les statistiques produisent généralement des détections plus fiables, les modèles de machine learning offrent un filet de sécurité pour capter les attaques qui échapperaient à des détections simples.

3. Visibilité et connaissance du contexte pour des actions rapides et ciblées

Une solution UEBA de pointe doit instantanément fournir aux équipes de sécurité la visibilité et les informations nécessaires pour évaluer rapidement les risques et détecter la présence de la moindre menace dans leur environnement. C'est là que les tableaux de bord et les visualisations jouent un rôle particulièrement important. La solution UEBA doit proposer un tableau de bord d'accueil affichant des indicateurs clés et différents volets afin de donner un aperçu de la position de sécurité actuelle de votre environnement. Quelques indicateurs indispensables :

- Menaces : nombre total de menaces actives dans votre environnement
- Anomalies : nombre total d'anomalies dans votre environnement
- Utilisateurs : nombre total d'utilisateurs, connus et inconnus, qui présentent un comportement anormal

- Appareils : nombre total d'appareils internes et externes présentant un comportement anormal
- Applications : nombre total d'applications anormales par rapport au nombre total d'applications

Ces tableaux de bord doivent également présenter des informations contextuelles détaillées sur tous les indicateurs clés. Par exemple, les analystes de sécurité trouveront les vues suivantes particulièrement intéressantes :

- Chronologie des menaces sur 7 jours, pour suivre les menaces et identifier les tendances récentes des activités malveillantes
- Dernières anomalies, pour voir les anomalies les plus récentes identifiées dans votre organisation
- Chronologie des anomalies sur 7 jours, pour identifier les anomalies récentes
- Traitement d'événements affichant le nombre d'événements actifs, pour vérifier que le processus de traitement se déroule comme prévu
- Tendance des événements sur 7 jours, pour identifier tout changement inattendu dans le traitement d'événements

Ces tableaux de bord et ces visualisations donneront aux analystes de sécurité les informations nécessaires pour lancer des workflows d'investigation en quelques clics.

4. Exploitation de plusieurs modèles de ML pour découvrir et éliminer les menaces

Les solutions UEBA doivent examiner les anomalies collectées à l'aide d'une série de modèles ML afin d'identifier les menaces qui méritent l'attention des analystes SOC. Au minimum, la solution doit inclure :

- **Des modèles de traitement par lot :** ces modèles et leurs règles d'anomalies associées s'appliquent aux données accumulées et stockées dans la solution UEBA. Ils analysent les données importées sur une période plus longue, les 24 dernières heures par exemple, et s'exécutent généralement pendant la nuit car ils doivent traiter de grandes quantités de données. Les cas d'utilisation tels que le signalement fonctionnent en mode mixte : le composant de flux identifie les événements d'intérêt qui peuvent être convertis en anomalies par les composants hors ligne.
- **Modèles d'analyse de sécurité :** une solution UEBA de pointe fournit des modèles capables d'établir le contexte de sécurité et de calculer des analyses. Ces modèles utilisent un éventail d'algorithmes de détection dédiés aux scénarios de sécurité. Pour améliorer la qualité de ces modèles, les algorithmes réévaluent les anomalies en affinant les règles d'action et de notation. Cela consiste notamment à classer les utilisateurs internes et externes et à effectuer une détection plus personnalisée reposant sur des règles de menace, des listes de supervision, des listes d'autorisation et de refus, et des tableaux de bord. Vous pouvez utiliser des règles d'action sur les anomalies pour gérer les anomalies existantes. Vous pourrez ainsi supprimer ou restaurer des anomalies, modifier leur score ou les ajouter à une liste de supervision. Vous pouvez également personnaliser les règles de notation des anomalies pour obtenir davantage de contrôle et de cohérence avec différents types d'anomalie.
- **Modèles de streaming :** ces modèles traitent les événements au fur et à mesure qu'ils se produisent, un atout de poids pour les scénarios d'utilisation où la séquence et la chronologie des événements sont cruciales. Les modèles de streaming analysent les données ingérées en temps réel et établissent l'impact de ces données sur une courte période, la dernière heure par exemple. Dans une solution UEBA, les modèles de streaming peuvent générer des anomalies, des indicateurs de compromission (IoC) ou des données analytiques.
- **Modèles de menaces :** ces modèles reposent sur les données et les anomalies du système. Les modèles de menaces prennent en compte l'agrégation des données, dont les données cataloguées par les modèles de streaming, pour générer des alertes de menaces. Les règles de menace de la solution UEBA peuvent signaler les menaces en recherchant des modèles d'anomalies spécifiques sur une fenêtre temporelle donnée. Chaque détection d'un modèle d'anomalie entraîne la création d'une alerte. Chaque règle de menace s'exécute selon un calendrier prédéfini, conformément à la nature de la règle.

  Il faut également avoir la possibilité de créer des règles de menace personnalisées pour identifier les menaces vérifiables présentes sur votre réseau. C'est particulièrement utile pour superviser la conformité de certaines activités aux politiques. Les menaces personnalisées peuvent s'appliquer aux utilisateurs, aux appareils ou aux sessions.

5. Intégration transparente avec le SIEM

Toute solution UEBA haut de gamme doit pouvoir s'intégrer de manière transparente à une solution SIEM de pointe. La combinaison du SIEM et de l'UEBA peut améliorer la performance du machine learning, la détection des comportements utilisateur anormaux, la corrélation enrichie par le contexte et les capacités d'investigation. Une solution intégrée va offrir une vue centralisée facilitant les investigations et la gestion des incidents. Elle va exploiter la puissance des deux produits pour obtenir davantage de contexte sur les anomalies touchant les utilisateurs, les appareils et les applications. Résultat : un système qui aide les équipes SOC à mieux détecter les menaces et à répondre rapidement à des alertes haute fidélité hiérarchisées.

Les capacités de détection des menaces d'une solution UEBA peuvent prolonger celles du SIEM, dont l'approche repose sur des recherches, des modèles et des règles. Sachez également qu'une solution UEBA de pointe utilise la corrélation et la détection de modèles basées sur le machine learning pour automatiser la détection de nombreuses menaces avancées : menaces internes, compromission de compte, abus de compte privilégié, déplacement latéral, exfiltration de données, etc. Un SIEM classique ne fournit pas cette fonctionnalité, ou alors sous une forme difficilement utilisable. De plus, un SIEM de pointe fournit généralement des mises à jour de contenu de sécurité dynamiques et récurrentes, grâces auxquelles les équipes de sécurité se tiennent constamment informées des dernières techniques de détection des menaces. En enrichissant les règles de corrélation et les recherches du SIEM, créées par des humains, grâce aux corrélations de menaces d'une solution UEBA haut de gamme exploitant le machine learning non supervisé, la détection, l'investigation et la prise en charge des menaces deviennent plus complètes et plus rapides.

Scénarios de menace traités par l'analyse du comportement des utilisateurs et des entités

Examinons plus en détail quelques applications de l'analyse du comportement des utilisateurs et des entités. Quels sont-ils ? Comment fonctionnent ces attaques ? Et quelle réponse apporte une solution d'analyse du comportement des utilisateurs et des entités ?

Compte utilisateur compromis

La compromission potentielle d'un compte utilisateur ou de service de confiance est un cas classique de menace interne. Les meilleures solutions d'analyse du comportement des utilisateurs et des entités doivent être capables d'identifier les cas de vol d'identifiants utilisateur et de savoir s'ils ont été utilisés par une entité autre que l'utilisateur autorisé. La détection de l'utilisation de comptes partagés et des abus de comptes génériques relève également de ce scénario d'utilisation.

Une excellente solution d'analyse du comportement des utilisateurs et des entités utilise la modélisation du comportement pour identifier toute déviation par rapport à l'activité normale de l'utilisateur afin de déterminer si le compte est exploité par une personne qui n'est pas son propriétaire légitime. La détection comprend l'identification d'activités Active Directory inhabituelles ou malveillantes : opérations sur soi-même, utilisateurs résiliés, comptes désactivés ou récupération de compte.

Machine compromise et infectée (logiciel malveillant)

Les solutions d'analyse du comportement des utilisateurs et des entités peuvent mettre en évidence les terminaux compromis, infectés par des logiciels malveillants ou qui se comportent de manière suspecte. Ce n'est pas la même situation que la compromission de compte utilisateur, dans le sens où une activité malveillante peut être détectée sur un hôte, mais pas nécessairement liée à un compte utilisateur spécifique. Par exemple, du trafic de commande et de contrôle (C&C) peut être identifié sur un système auquel aucun utilisateur n'est connecté actuellement.

Une solution haut de gamme d'analyse du comportement des utilisateurs et des entités utilise une modélisation basée sur le comportement pour identifier les activités de logiciels malveillants, quel que soit le mécanisme de transmission de l'infection initiale. Il existe plusieurs techniques de détection : le suivi des modifications dans les modèles de communication des périphériques, la nature des communications avec des domaines ou des adresses IP externes, et les caractéristiques de ces domaines.

Exfiltration des données

Des utilisateurs autorisés peuvent mener une exfiltration de données non autorisée ou malveillante, même si votre équipe a déjà la capacité de détecter les comptes et les terminaux compromis. Une solution haut de gamme d'analyse du comportement des utilisateurs et des entités peut détecter la perte ou le vol de données privées et confidentielles de l'entreprise sur plusieurs vecteurs de menaces : infrastructure de sécurité réseau (pare-feu et proxys), stockage cloud en ligne, stockage connecté (USB) et e-mail.

Déplacement latéral

Un déplacement latéral effectué par un initié de confiance implique qu'un utilisateur analyse et étende son accès à plusieurs ressources. Des techniques de détection comme la rareté d'un accès ou une utilisation croissante de certaines ressources permettent d'identifier les mouvements latéraux. Les ressources en question peuvent être des machines, des partages de fichiers réseau ou des dossiers de dépôt (Box). Les accès peuvent prendre différentes formes : analyses de réseau, connexions par force brute et connexions légitimes. Une bonne solution d'analyse du comportement des utilisateurs et des entités doit savoir détecter les mouvements latéraux en comparant les anomalies à une base de référence.

Comportements suspects et menaces inconnues

Les solutions d'analyse du comportement des utilisateurs et des entités sont très efficaces pour détecter les scénarios inconnus : elles identifient les anomalies en observant les déviations dans l'activité d'un utilisateur ou d'un appareil par rapport à sa base de référence ou celle de son groupe de pairs, les activités suspectes ou malveillantes et les alertes provenant d'outils externes, puis les corrèle pour établir la menace. Souvent, une activité de compte suspecte ou une menace inconnue nécessite une investigation plus approfondie. Les menaces inconnues peuvent prendre de nombreuses formes : publicité malveillante, compromission de compte, utilisation abusive de compte, violations de politique et mauvaise configuration. Ces menaces sont souvent utilisées par les solutions UEBA pour la création de contenu. Une fois qu'un scénario inconnu a été détecté, ce scénario peut ensuite être formalisé sous forme de règles de recherche de corrélation ou de menace à des fins de détection déterministe.

Utilisation abusive du compte

L'utilisation abusive des privilèges de superutilisateur, qu'elle soit accidentelle ou délibérée, présente des risques critiques en matière de conformité et de confidentialité, avec des impacts financiers et de réputation potentiellement lourds. Une solution haut de gamme d'analyse du comportement des utilisateurs et des entités établit le comportement régulier de chaque compte (pas seulement des comptes utilisateur) et identifie toute anomalie pouvant indiquer une utilisation excessive, un accès rare, un sabotage potentiel ou une dissimulation de traces. Plus l'activité des utilisateurs s'écarte de celle de son groupe de pairs et du profil de l'entreprise, plus la confiance de la solution UEBA augmente. Plus la confiance est élevée, plus le risque est élevé. La solution va, entre autres, détecter les accès à des connexions VPN ou interactives provenant de comptes de service, l'espionnage de données, la suppression de logs d'audit et l'accès à des informations confidentielles.

Intelligence contextuelle

Les meilleures solutions d'analyse du comportement des utilisateurs et des entités acquièrent un maximum de connaissances sur les utilisateurs et les entités de l'organisation afin d'identifier les anomalies pouvant traduire la présence de menaces. Ces informations sont extrêmement utiles pour les analystes chargés de trier les alertes et d'investiguer les incidents. Si un analyste soupçonne qu'un terminal a été compromis, par exemple, il peut utiliser une solution UEBA pour en savoir plus sur les utilisateurs de cet ordinateur, leur comportement habituel et même le rôle de ce terminal dans le réseau. Par exemple, s'agit-il d'un serveur ou d'un poste de travail ? Est-il utilisé pour l'administration du système ou pour des fonctions métiers ?

Splunk entre en jeu

Splunk User Behavior Analytics (UBA) aide les organisations à détecter les menaces connues, inconnues et cachées parmi les utilisateurs, les terminaux et les applications. Malgré son nom « User Behavior Analytics », Splunk UBA analyse à la fois les utilisateurs et les entités en s'appuyant sur des bases de comportement multidimensionnelles, l'analyse de groupes de pairs dynamiques et le machine learning non supervisé. Splunk UBA peut ainsi détecter rapidement les comportements anormaux (comptes et appareils compromis ou mal utilisés, vol d'adresses IP ou exfiltration de données) et les éliminer.

Grâce au machine learning, Splunk UBA déduit des séquences et des modèles pour chaque anomalie, en plus d'autres indicateurs, afin de filtrer et identifier les menaces prioritaires, critiques et exploitables.

Dans ce déluge d'informations, ce sont ces menaces qui représentent le risque le plus probable pour votre entreprise. Splunk User Behavior Analytics améliore les workflows des analystes et chasseurs de sécurité, tout en nécessitant une administration minimale, et s'intègre aux infrastructures existantes pour localiser les menaces.

Vous voulez détecter les menaces avancées ? Splunk UBA peut vous aider à repérer les anomalies et les menaces inconnues qui échappent aux outils de sécurité traditionnels. Vous voulez améliorer la productivité de votre SOC ? Splunk UBA assemble automatiquement des centaines d'anomalies en une seule menace pour simplifier et accélérer les investigations sur les incidents. Vous voulez accélérer la recherche des menaces ? Utilisez les capacités d'investigation approfondie de Splunk UBA et ses puissantes références comportementales pour évaluer n'importe quelle entité, anomalie ou menace.

Détectez les menaces avancées et les comportements anormaux grâce au machine learning

Splunk UBA utilise des algorithmes de machine learning non supervisé pour établir les comportements de référence des utilisateurs, des appareils et des applications, puis recherche les déviations pour mettre en évidence les menaces inconnues :

- Compte utilisateur compromis : toute déviation par rapport à l'activité normale de l'utilisateur, signe qu'un compte est exploité par une personne autre que son propriétaire légitime.
- Machine compromise : identification des terminaux du réseau qui ont été compromis ou infectés par des logiciels malveillants, ou bien qui se comportent de manière suspecte.
- Exfiltration de données : détection de la perte ou de la transmission de données privées et confidentielles vers l'extérieur de l'entreprise sur plusieurs vecteurs de menaces : pare-feux et proxys, stockage cloud, stockage connecté ou messagerie électronique.
- Déplacement latéral : un utilisateur interne de confiance analyse et étend son accès à plusieurs ressources.
- Utilisation abusive du compte : utilisation abusive, accidentelle ou délibérée, des privilèges de superutilisateur.

Gagnez en visibilité et obtenez des informations contextuelles riches pour évaluer rapidement les risques et agir rapidement et fermement

Splunk User Behavior Analytics met en évidence les différentes phases d'attaque d'une menace pour donner aux analystes de sécurité une image complète de la cause profonde, de l'étendue, de la gravité et de la chronologie de l'attaque. Cette vue fortement contextualisée permet aux analystes d'évaluer rapidement l'impact et de prendre des décisions éclairées en toute confiance. L'analyse de graphe et de kill-chain permet de mener une investigation approfondie sur un utilisateur, une entité, une anomalie ou une menace et d'en extraire plus rapidement des informations.

Simplifiez et rationalisez les investigations et les workflows de prise en charge des incidents pour accroître l'efficacité du SOC.

Splunk User Behavior Analytics réduit automatiquement des milliards d'événements bruts à quelques dizaines de menaces qui peuvent être examinées rapidement. Il évite à votre équipe de professionnels hautement qualifiés en sécurité et en data science de perdre son temps à mener des investigations manuelles et fastidieuses. En filtrant les alertes avant qu'elles ne parviennent à l'équipe SOC, Splunk UBA permet aux analystes de sécurité de se concentrer sur les menaces les plus urgentes et les plus complexes.

Associez le SIEM à l'analyse du comportement des utilisateurs et des entités pour une protection complète

Splunk User Behavior Analytics donne des informations sur les anomalies et les menaces multi-entités en se basant sur le comportement. Splunk Enterprise Security s'appuie sur des règles de corrélation et des recherches. En combinant les deux, les équipes de sécurité peuvent mettre en place une défense robuste et à grande échelle contre les menaces les plus sophistiquées. Splunk UBA transmet automatiquement les informations sur les menaces à Splunk Enterprise Security pour produire une vue centralisée des incidents et un workflow d'investigation de bout en bout.

Pour commencer

Vous voulez savoir comment l'analyse du comportement des utilisateurs et des entités peut moderniser votre SOC et vous aider à découvrir et à éliminer les menaces furtives les plus avancées ? Rendez-vous sur la page Splunk UBA, suivez la visite guidée du produit ou échangez dès maintenant avec un expert en sécurité Splunk.

splunk>

23-490251-Splunk-The Essential Guide to User and Entity Behavior Analytics -EB-106