Le Guide essentiel de l'approche

Zero Trust

splunk>

turn data into doing™

Sommaire

Aujourd'hui plus que jamais, les entreprises se tournent vers une stratégie Zero Trust pour sécuriser leurs données et leurs systèmes. Quels que soient la taille et le secteur d'une entreprise, l'approche Zero Trust est indispensable en raison de la pandémie de COVID-19. Les failles de sécurité majeures (comme SolarWinds), la migration vers le cloud et l'expansion permanente de la surface d'attaque rendent ce changement d'approche d'autant plus crucial.

Mais ce type d'initiative peut sembler intimidant. Surtout lorsqu'il s'agit de repenser la façon de prendre en charge la sécurité de l'ensemble de l'entreprise, en pensant à chaque périphérique, application et utilisateur qui y est connecté. Pour compliquer davantage les choses, l'approche Zero Trust ne se limite pas uniquement à l'IT traditionnelle, et s'étend aux technologies opérationnelles et systèmes de contrôle industriel (OT/ICS) ainsi qu'à l'Internet des objets (IoT), deux points de vulnérabilité populaires auprès des pirates.

La bonne nouvelle ? Un modèle Zero Trust peut radicalement améliorer la posture de sécurité de votre entreprise *et* minimiser les efforts opérationnels en cessant de faire de la protection périmétrique la seule ligne de défense. Au lieu de suivre les méthodes traditionnelles, l'approche Zero Trust établit un certain niveau de confiance à chaque point d'accès, pour protéger efficacement les utilisateurs, les actifs et les ressources. Il ne faut pas pour autant renoncer à sécuriser le périmètre. Il s'agit plutôt d'un virage organisationnel dans l'approche de la protection des actifs de base.

En bref : Zero Trust n'est pas *seulement* un cadre architectural. C'est un état d'esprit qui pousse les organisations à repenser ce qui est supervisé, trié et corrigé. Dans ce guide essentiel, nous allons étudier les forces motrices qui imposent une stratégie Zero Trust, ce que cette stratégie implique, comment la mettre en œuvre et, en fin de compte, comment réinventer ce que signifie vraiment être en sécurité.

Qu’est-ce que le modèle Zero Trust ?

Le principe fondamental de l’approche Zero Trust consiste à sécuriser les données d’une entreprise où qu’elles soient, tout en permettant uniquement *aux utilisateurs et aux entités légitimes* d’accéder aux ressources et actifs qui les concernent. Dans cet état d’esprit, chaque utilisateur, périphérique et service qui nécessite un accès au réseau d’une entreprise est considéré comme hostile jusqu’à preuve du contraire.

En d’autres termes, la clé consiste à comprendre qui demande un accès, de quel périphérique provient la demande, puis de rapprocher ces informations des stratégies d’accès par application ou ressource. Cela revient à appliquer un principe de liste blanche pour accorder les accès, en fonction de l’appareil, des identifiants et du comportement de l’employé. L’authentification doit être appliquée en permanence au niveau du périphérique et de l’utilisateur pour chaque session, ce qui garantit une autorisation continue et adaptative à une échelle granulaire.

Pour voir les choses plus en détail, un programme de sécurité Zero Trust réussi doit :

- partir du principe que le réseau est toujours hostile ;
- accepter l’idée que des menaces internes et externes soient toujours présentes sur le réseau ;
- savoir que l’emplacement d’une localité de réseau ne suffit pas à accorder la confiance ;
- authentifier et autoriser chaque périphérique, utilisateur et flux réseau ;
- mettre en œuvre des politiques dynamiques et calculées à partir du plus grand nombre possible de sources de données.

Prenons l’exemple d’un employé autorisé à utiliser le système de gestion de dossiers d’une entreprise à partir d’un appareil qu’on vient de lui remettre. L’employé fait une demande à partir de cet appareil et reçoit un accès. Plus tard, il télécharge un pilote sur un site web, pensant être utile. Comme l’appareil est supervisé en permanence dans le cadre d’une stratégie Zero Trust, la mise à jour est signalée.

Ce composant nouvellement ajouté a modifié la configuration, et donc le score de confiance, de l’appareil en question. Maintenant, lorsque l’employé tente de se connecter au système, son accès peut être refusé ou rétrogradé, selon son nouveau score de confiance et la politique associée. Cela montre comment l’application de plusieurs facteurs (dans ce cas, les scores combinés de l’utilisateur, de l’appareil et des ressources) aide les équipes de sécurité à réduire dynamiquement les risques pesant sur les ressources de l’entreprise. Un système Zero Trust est capable de prendre en compte l’évolution des conditions pour une évaluation et une protection continues.

L'évolution de l'approche Zero Trust

Avant que l'approche Zero Trust ne soit définie pour la première fois par Forrester en 2010, les spécialistes de la sécurité ont suivi un modèle de segmentation basé sur le réseau et reposant sur les solutions traditionnelles de sécurité réseau. Cette stratégie consiste à renforcer le périmètre, ou à bâtir des remparts métaphoriques autour du réseau d'une entreprise, pour abriter toutes ses précieuses ressources et données. Mais si un pirate parvient à pénétrer le réseau et à franchir le périmètre, il peut alors, en toute liberté, se déplacer latéralement dans le réseau et dans les systèmes connectés, compromettant les actifs et causant des dommages irréversibles.

Abandonnez le mythe du périmètre

Finalement, les équipes de sécurité ont commencé à passer d'une approche centrée sur le réseau à une approche centrée sur l'idée que tout périphérique, utilisateur ou système, qu'il soit interne ou externe à l'entreprise, ne doit jamais être implicitement approuvé et que l'accès à toutes les ressources doit être explicitement authentifié et autorisé. Cependant, jusqu'à récemment, c'était beaucoup plus facile à dire qu'à faire. Certaines technologies manquaient simplement des fonctions d'intégration nécessaires : elles limitaient donc la capacité d'une entreprise à superviser de manière centralisée et globale la sécurité de l'ensemble de ses ressources, créant une fragmentation supplémentaire et nécessitant une mise en œuvre détaillée par les ingénieurs de sécurité.

Aujourd'hui, d'innombrables technologies s'articulent autour du contrôle d'accès, un ensemble de règles pour déterminer qui doit avoir accès à un emplacement restreint et/ou à des informations critiques. Une architecture Zero Trust peut réunir ces systèmes et réduire la complexité associée à la gestion indépendante de multiples contrôles.

Ces technologies sont nombreuses, mais en voici quelques exemples importants :

- la gestion des identités et des accès (IAM) ;
- l'authentification multifacteurs (MFA) ;
- la prévention des pertes de données (DLP) ;
- les courtiers de sécurité d'accès au cloud (CASB) ;
- la gestion des droits d'accès à l'infrastructure cloud (CIEM).

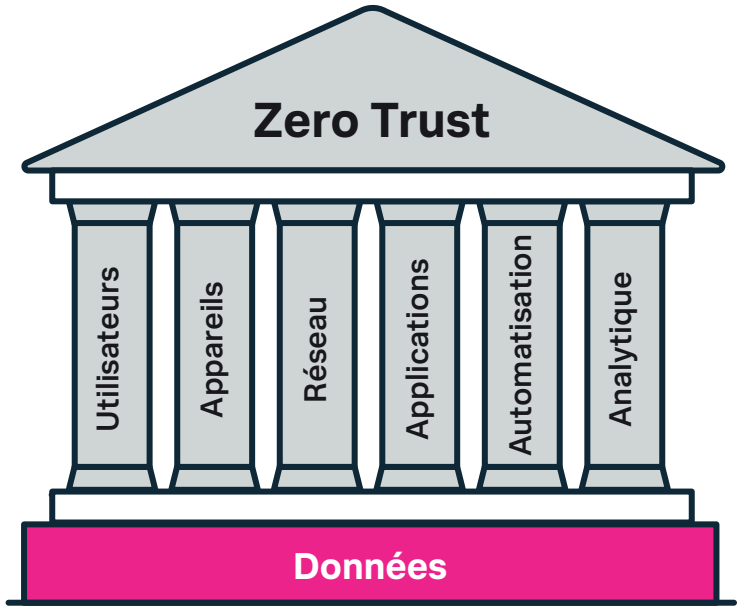
Grâce à ces avancées, l'approche Zero Trust est devenue plus facile à mettre en œuvre. La pandémie de COVID-19 a également poussé les organisations et les entreprises du monde entier à accélérer leur transformation numérique. Du jour au lendemain, les employés ont été contraints de travailler à distance, mettant à rude épreuve l'infrastructure IT et de sécurité. Appuyée par le défi d'un périmètre en pleine dissolution et d'une surface d'attaque croissante, l'approche Zero Trust est devenue un impératif mondial absolu.

Le modèle Zero Trust

L'American Council for Technology and Industry Advisory Council (ACT-IAC), un partenariat public-privé à but non lucratif voué à l'amélioration du gouvernement par le biais des technologies de l'information, établit les six piliers d'un modèle de sécurité Zero Trust, chacun reposant sur des données.

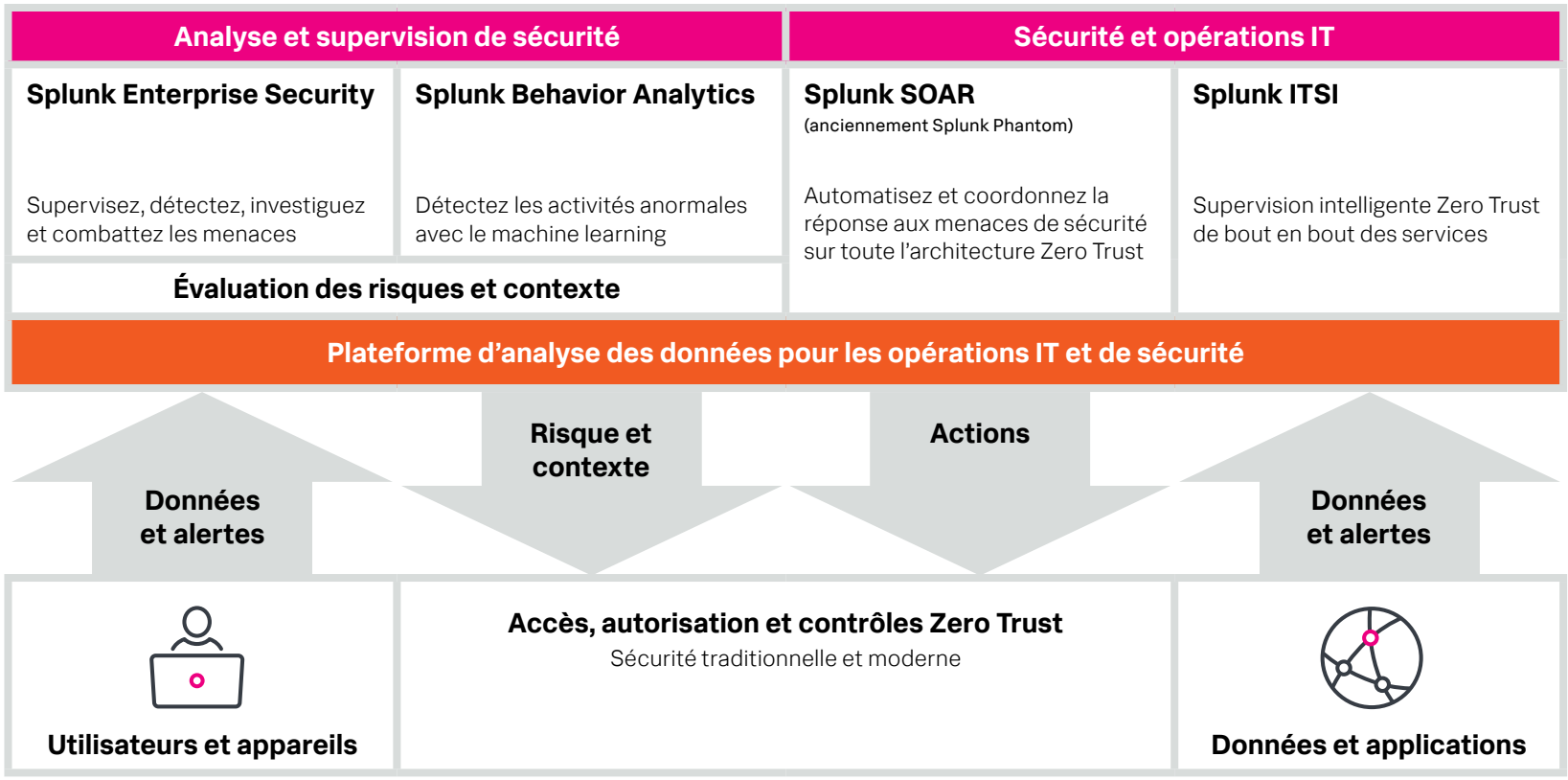
Ils se résument de la façon suivante :

- **Utilisateurs :** authentifier en permanence les utilisateurs de confiance, superviser et vérifier continuellement la fiabilité des utilisateurs pour gérer leurs accès et leurs privilèges.
- **Appareils :** mesurer la position de cybersécurité en temps réel et la fiabilité des périphériques.
- **Réseau :** segmenter, isoler et contrôler le réseau, y compris les réseaux définis par logiciel, les réseaux étendus définis par logiciel et les technologies basées sur Internet.
- **Applications :** sécuriser et gérer correctement la couche applicative, ainsi que les conteneurs et les machines virtuelles.
- **Automatisation :** l'automatisation, l'orchestration et la réponse de sécurité (SOAR) permettent aux entreprises d'automatiser les tâches sur l'ensemble des produits par le biais de workflows et d'effectuer une supervision interactive des utilisateurs finaux.
- **Analytique :** les outils de visibilité et d'analyse comme la gestion des informations et des événements de sécurité (SIEM), l'analyse de sécurité avancée et l'analyse du comportement des utilisateurs et des entités (UEBA) permettent aux experts de la sécurité d'observer ce qui se passe et d'orienter leurs défenses en conséquence.



Votre aide-mémoire Zero Trust pratique

☐	Un modèle Zero Trust doit autoriser et authentifier l'accès des utilisateurs à tous les actifs et ressources, et l'accès doit être accordé en fonction de la politique d'entreprise correspondante, session par session.
☐	Les contrôles Zero Trust doivent être identifiés et alignés sur vos systèmes, utilisateurs et données. Ils doivent être pris en compte sous deux angles :
	☐ Contrôles de sécurité pour la sécurisation de l'infrastructure interne/cloud, des réseaux, des systèmes, des applications et des données, qui sont parfois désignés comme « objets ».
	☐ Contrôles de sécurité pour la protection et l'autorisation des utilisateurs et des points de terminaison lors de l'accès aux ressources. Ces contrôles doivent également inclure un accès administratif, et s'appliquent aux « sujets ».
☐	Un ensemble commun de politiques, de pratiques et de protocoles doit être mis en place pour gérer l'identité et le score de confiance des utilisateurs et des appareils sur tous les systèmes, y compris externes (les logiciels en tant que service notamment).
☐	La gestion des contrôles Zero Trust doit être unifiée et l'accès dynamique de bout en bout doit être configuré en fonction de la logique métier, et non des règles de sécurité traditionnelles (comme les contrôles basés sur l'IP).
☐	L'analyse de données de bout en bout doit être mise en place, afin d'assurer la supervision et la détection des menaces sur l'ensemble de l'architecture, en prenant en charge les besoins des opérations IT et de sécurité.
☐	Une position de sécurité centralisée est adoptée, avec un profilage des risques contextualisé et une logique de stratégie avancée pour l'autorisation d'accès.
☐	Les contrôles et processus de sécurité existants doivent être examinés, de même que leur adéquation et leur compatibilité au sein de l'architecture Zero Trust à plus grande échelle.



Maintenant que vous maîtrisez l'histoire et les principes de base de l'approche Zero Trust, nous pouvons continuer. Dans les sections suivantes, nous verrons comment la création d'un centre d'opérations de sécurité (SOC) moderne peut assurer la supervision de la sécurité selon le modèle Zero Trust, et comment Splunk peut aider les entreprises à atteindre leurs objectifs Zero Trust sans délai.

Le parcours d'analyse de données Splunk pour une approche Zero Trust

Dans la démarche d'adoption d'une stratégie Zero Trust, il est essentiel de superviser, de détecter et d'investiguer les incidents de sécurité liés aux contrôles et politiques Zero Trust, en particulier les protections en place pour les utilisateurs, les systèmes, les applications et les données.

Après de nombreuses années passées à aider les clients à mettre en œuvre des solutions d'analyse des données, en plus d'examiner les bonnes pratiques du secteur et l'expérience collective de Splunk, Splunk a développé ce que nous aimons appeler le parcours d'analyse des données de sécurité.

Ce modèle de maturité décompose le parcours de sécurité d'une entreprise en étapes distinctes. L'objectif est que chaque étape couvre des objectifs spécifiques, tout en permettant des améliorations incrémentielles et itératives avant de passer à la phase suivante de développement. Bien que ce parcours soit axé sur les résultats de sécurité, il s'aligne également sur le développement de capacités de supervision IT par la réutilisation et le rehashage des données.

Cette approche est parfaitement adaptée aux objectifs suivants : 1. Aider les opérations IT et de sécurité à mieux s'aligner sur une stratégie Zero Trust, et 2. Construire un SOC moderne qui prend en charge une architecture Zero Trust et comble les lacunes existantes. Les sections suivantes décrivent chaque phase du parcours d'analyse des données ainsi que les étapes correspondantes, afin que vous puissiez répondre aux exigences Zero Trust parallèlement à celles de vos opérations IT et de sécurité.

Le parcours Splunk d'analyse des données de sécurité

ÉTAPE 6

Détection avancée
Mettez en œuvre des mécanismes de détection sophistiqués en exploitant le machine learning.

ÉTAPE 5

Automatisation et orchestration
Mettez en place une capacité cohérente et reproductible d'opérations de sécurité.

ÉTAPE 4

Enrichissement
Augmentez les données de sécurité à l'aide de sources d'informations pour mieux comprendre le contexte et l'impact d'un événement.

ÉTAPE 3

Expansion
Collectez des sources de données supplémentaires, comme des métadonnées sur l'activité des points de terminaison et le réseau pour faciliter la détection des attaques avancées.

ÉTAPE 2

Normalisation
Appliquez une taxonomie de sécurité standard et ajoutez des données d'actifs et d'identité.

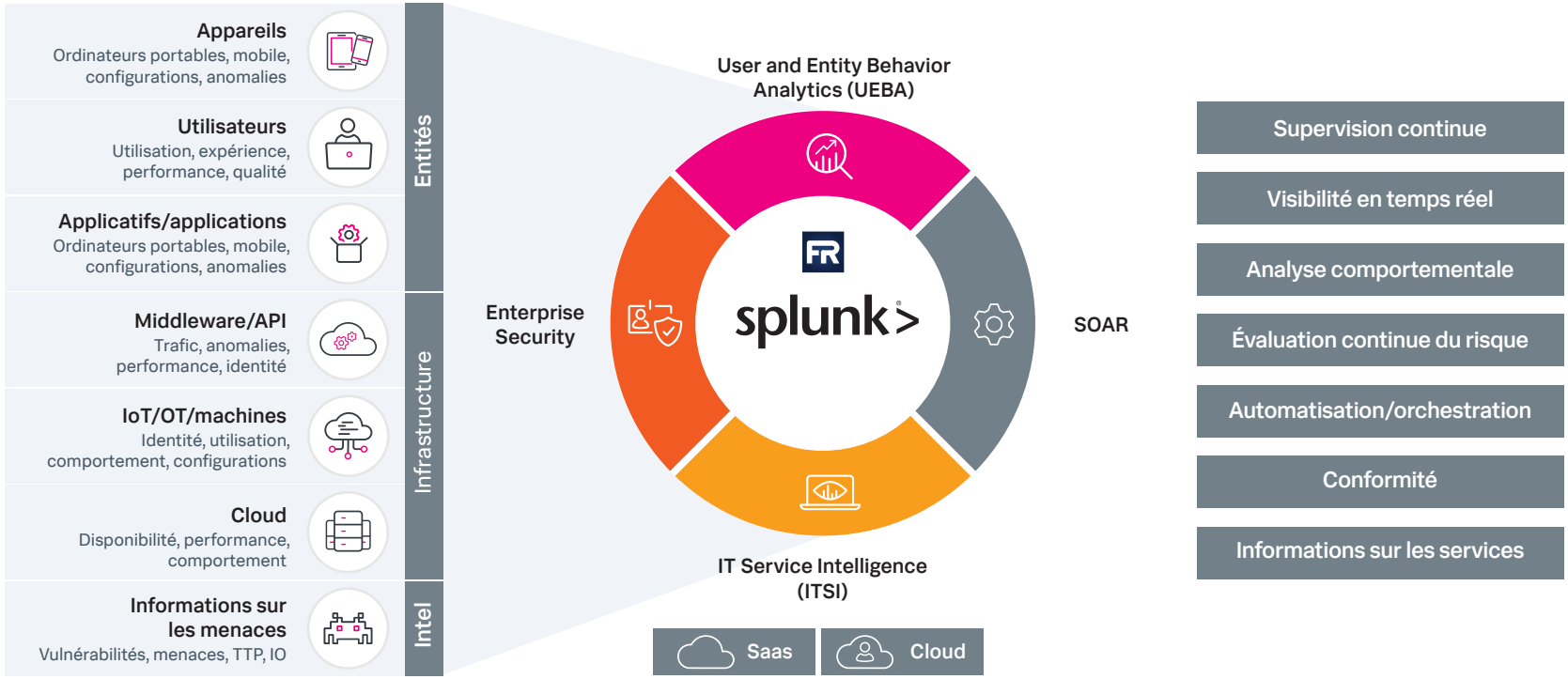
ÉTAPE 1

Collecte
Collectez les journaux de sécurité de base et autres données machine de votre environnement.

À chaque étape de votre parcours Zero Trust, nous verrons comment notre suite de produits s'aligne sur les différentes exigences de sécurité et de supervision IT propres à ce modèle. Ces produits sont les suivants :

- Splunk Enterprise : plateforme d'analyse et d'investigation des données
  - Plateforme évolutive d'analyse des données, qui prend en charge les scénarios d'utilisation de l'IT, de la sécurité et de la lutte contre la fraude pour les architectures Zero Trust.
  - Capacité à acquérir une large gamme de données structurées et non structurées.
  - Écosystème de partenaires complet, qui inclut des solutions Zero Trust pour prendre en charge l'intégration des systèmes, ainsi que l'importation et la normalisation rapides des sources de données.
- Splunk Enterprise Security : un nouveau système de gestion des événements et des informations de sécurité (SIEM)
  - Bibliothèque complète de scénarios de détection et de supervision de la sécurité, assurée par Splunk Security Essentials (SSE) et Enterprise Security Content Update (ESCU).
  - Des frameworks clés pour soutenir l'enrichissement et la contextualisation des données d'identité et de ressources, l'évaluation des risques et la sécurité, afin de soutenir les objectifs Zero Trust.
  - Le système d'alerte basée sur le risque (RBA) permet d'améliorer l'évaluation des risques et la détection multi-indicateurs, conformément au framework MITRE ATT&CK. Examine les contrôles Zero Trust pour repérer une séquence d'activités pouvant indiquer un comportement malveillant.
- Splunk User and Entity Behavior Analytics (UEBA)
  - Machine learning non supervisé prêt à l'emploi, pour une détection avancée des comportements et une résolution automatique de l'identité.
- Splunk SOAR pour l'orchestration, l'automatisation et la réponse de la sécurité (anciennement Splunk Phantom)
  - Gestion complète des cas, investigation des incidents, orchestration et automatisation de la réponse aux incidents de sécurité et de service sur une architecture Zero Trust.
- Splunk IT Service Intelligence (ITSI)
  - Supervision de bout en bout des contrôles Zero Trust et de l'infrastructure sous-jacente des applications et services associés.

Vue d'ensemble de la solution Splunk pour les opérations IT et de sécurité Zero Trust



Étape 1 : Collectez toutes les données utiles

Tout d'abord, identifiez les actifs les plus critiques de votre organisation, en particulier ceux que vous devez protéger et superviser par ordre de priorité. Une fois que vous aurez trié vos actifs, vous saurez bien mieux où affecter vos ressources et de quelles sources extraire les données en premier.

Comme l'approche Zero Trust s'appuie sur de nombreux types de technologies, il est fort probable que votre organisation utilise déjà certains de ces systèmes. Cela va constituer une source importante de données pour la supervision IT et celle de la sécurité, et la base même d'un programme Zero Trust complet de bout en bout.

Voici quelques exemples de ces technologies :

- pare-feux nouvelle génération (NGFW) ;
- solutions de réseau défini par logiciel (SDN) et micro-segmentation ;
- courtiers de sécurité d'accès au cloud (CASB) ;
- accès à distance ;
  - réseau privé virtuel (VPN) ;
  - infrastructures de bureaux virtuels (VDI) ;
  - accès ZT (ZTA) ;
- gestion des accès aux identités (IAM) et services d'annuaire ;
- authentification multifacteurs (MFA) ;
- gestion des authentifications privilégiées (PAM) ;
- détection des points de terminaison et réponse (EDR) ;
- solutions de position de sécurité (gestion des correctifs et des vulnérabilités, par exemple) ;
- proxy web, filtrage web et services d'accès sécurisé au Web ;
- prévention des pertes de données (DLP) ;
- frontière de service d'accès sécurisé (SASE) ;
- solutions de gestion unifiée des points de terminaison (UEM) et de gestion des périphériques mobiles.

Les éléments qui constituent l'infrastructure sous-jacente des systèmes et des services, comme le stockage et les réseaux, ainsi que les composants qui prennent en charge les fonctions administratives IT, sont également des sources de données importantes et doivent être pris en compte au cours de cette phase.

Quelques exemples :

- **Réseau :** infrastructure réseau du datacenter et du cloud, comme les switches, les routeurs, les équilibreurs de charge, ainsi que tous les services réseau virtualisés.
- **Stockage :** les systèmes et services de stockage dans le cloud et le datacenter, tels que les baies de stockage, les disques système, le stockage en réseau (NAS/SAN) et les services de stockage dans le cloud.
- **Calcul :** ressources de datacenter et de cloud computing, notamment la supervision des systèmes de traitement physique et virtualisé, et celle des systèmes d'exploitation associés.
- **Administration :** systèmes et applications prenant en charge des fonctions administratives telles que les systèmes de supervision, les hôtes Jump, l'authentification administrative et le contrôle des accès privilégiés.

La charge de travail peut paraître importante, mais un élément clé du processus d'analyse des données de Splunk consiste à prendre des mesures incrémentielles en fonction de chaque système ou service, ainsi que du scénario d'utilisation spécifique que vous implémentez à ce moment-là. En identifiant et en définissant vos ressources et entités les plus critiques, vous formez la base même de la contextualisation et de la hiérarchisation des alertes d'incidents IT et de sécurité. Et lorsque vous allez élargir vos sources de données, vous aurez la possibilité de réutiliser ces données au fil de votre progression sur la courbe de maturité.

Étape 2 : Comprenez et contextualisez vos données

La contextualisation de vos données est la clé de toute stratégie Zero Trust. Pour comprendre vos données, vous devez implémenter une taxonomie standard dans toutes les sources de données, sans quoi le rapport signal-bruit sera extrêmement médiocre. La création d'une taxonomie éliminera une grande part de confusion, surtout lorsque vous progresserez dans votre parcours de sécurité.

Prenons l'exemple des fournisseurs de pare-feux, qui utilisent différents formats de logs et différentes structures de données selon les systèmes. Pour permettre une supervision centralisée, les données des logs du pare-feu doivent être structurées sous une forme qui normalise les noms et les valeurs des champs, en les inscrivant dans un format cohérent.

Structurer ou ne pas structurer ? Telle est la question

Splunk a développé un modèle de données unifié (CIM), une approche ouverte et extensible pour créer une taxonomie commune. Le CIM Splunk offre un moyen de structurer et de standardiser les noms et les valeurs des champs, qui sont extraits des données brutes puis transformés en modèles de données couvrant un large éventail de catégories. Avec Splunk, cette opération est effectuée après l'importation, sans modification des données brutes elles-mêmes.

Vous pouvez donc continuer à mettre à jour les structures de données en fonction de l'évolution de vos besoins, *sans* modifier vos données brutes ni être obligé de les réimporter. Autre avantage, cette approche se prête à l'accélération des modèles de données : vous pouvez accélérer des ensembles de données à l'aide d'une recherche pivot, ce qui augmente les performances de recherche sur les données structurées. En fin de compte, vous obtenez de manière rapide et prévisible les résultats qui garantissent la santé globale de votre modèle Zero Trust.

Le CIM Splunk prend en charge ces fonctionnalités natives de supervision et de détection au sein de Splunk Enterprise Security (ES) et peut être appliqué à toutes vos sources de données dédiées Zero Trust. L'intégration et la normalisation des données sont également prises en charge par notre écosystème de partenaires et d'utilisateurs Splunk, qui met une gamme complète d'extensions Splunk à la disposition des utilisateurs.

En conclusion ? Les extensions Splunk prennent en charge d'innombrables sources de données Zero Trust et sont continuellement mises à jour pour proposer des fonctionnalités améliorées ou innovantes.

La nouvelle norme(alisation)

Nous pouvons maintenant commencer à implémenter des scénarios d'utilisation conçus pour les données normalisées. La bibliothèque de cas d'utilisation fournie par Splunk Security Essentials (SSE) constitue un excellent point de départ pour les détections de sécurité. SSE propose une gamme complète de scénarios correspondant à chaque phase du processus d'analyse de la sécurité.

Mieux encore, il existe maintenant une nouvelle catégorie dans SSE qui identifie et mappe les scénarios d'utilisation Zero Trust à chaque étape de votre parcours en s'alignant sur le framework MITRE ATT&CK. Le framework MITRE ATT&CK fournit une base de connaissances étendue sur les tactiques et techniques des menaces réelles, et il est largement utilisé par les équipes de sécurité.

Nous avons fait de MITRE ATT&CK une arme

En évaluant les menaces qu'une stratégie Zero Trust vise à prévenir, nous avons identifié une liste complète de scénarios de sécurité, basée sur les tactiques MITRE ATT&CK. Compte tenu de la complexité et de la portée d'une implémentation complète de l'approche Zero Trust, cela peut aider les entreprises à enrichir une approche basée sur les contrôles avec des cas d'utilisation de détection de sécurité et de supervision adaptés au modèle Zero Trust.

N'oubliez pas : ces conseils doivent être envisagés dans le contexte d'une stratégie plus large de supervision de la sécurité, car de nombreux autres types de menaces *peuvent* et *vont* se manifester dans des situations particulières.

Les tactiques MITRE ATT&CK ci-dessous ont été utilisées pour classer une partie des principaux scénarios de détection de sécurité de SSE dans une optique Zero Trust :

- **Accès initial :** l'adversaire tente d'entrer dans votre réseau.
- **Persistance :** l'adversaire tente de maintenir sa présence.
- **Acquisition de privilèges :** l'adversaire tente d'obtenir des autorisations de niveau supérieur.
- **Accès aux identifiants :** l'adversaire tente de voler des noms de compte et des mots de passe.
- **Déplacement latéral :** l'adversaire tente de se déplacer dans votre environnement.
- **Exfiltration :** l'adversaire tente de voler des données.

Les scénarios d'utilisation suivants peuvent s'appliquer à la deuxième étape de votre processus de sécurité (normalisation des données) et s'appuient sur des sources de données de base telles que l'authentification, le réseau et les points de terminaison (ces sources ont été intégrées à la première étape) :

- modifications de la gestion des comptes ;
- création de nouveaux comptes ;
- modifications apportées aux stratégies ou aux contrôles de sécurité ;
- activité d'authentification par force brute ;
- effacement des logs d'administration ou de sécurité ;
- modifications non autorisées de la configuration du système.

La normalisation des données faisant partie de cette étape, nous pouvons nous tourner vers Splunk Enterprise Security pour superviser et générer des rapports sur les activités Zero Trust. Il s'agit notamment des activités suivantes :

- présence de programmes malveillants sur les points de terminaison et les serveurs, et supervision des changements de configuration du système ;
- vulnérabilité des points de terminaison et des serveurs et gestion des correctifs ;
- accès utilisateur et gestion des comptes ;
- supervision de l'activité web des utilisateurs ;
- supervision du trafic réseau.

Nous pouvons maintenant commencer à intégrer des informations comme le profil de risque des systèmes que nous protégeons, ainsi que le contexte utile entourant l'identité des utilisateurs. C'est un élément clé de l'analyse de la sécurité, car il constitue la base de l'évaluation des risques et de la hiérarchisation des alertes de sécurité. Et comme vous avez déjà identifié les actifs et les entités que vous devez protéger (nous l'avons vu à la première étape), vous pouvez utiliser ces informations pour obtenir une définition supplémentaire.

Exemples d'informations contextuelles importantes :

- **Profil de risque d'actif :** quel est l'impact commercial d'un incident affectant cet actif ? Quelle est la probabilité qu'un incident affecte cet actif ? Quelle est la position de sécurité de cet actif ? Quelle est la sensibilité ou l'importance des données traitées ou contenues dans ce système ? Quels types d'utilisateurs accèdent à, ou utilisent généralement ce système ?
- **Profil de risque d'identité :** quelle est l'importance de cette identité ? S'agit-il d'un compte de service, d'un compte administratif, d'un compte d'utilisateur de niveau cadre ou d'un compte de sous-traitant ? Ce compte est-il plus susceptible d'être visé ou est-il intrinsèquement peu digne de confiance ? Quel sera l'impact si cette identité est compromise ? L'utilisateur présente-t-il un risque de fuite ?

Le framework d'actifs et d'identités inclus dans Splunk ES fait partie intégrante de cette étape d'analyse et constitue la base même de l'évaluation des risques. Chaque actif ou identité connecté à ES conserve un enregistrement chronologique, en fonction des événements de sécurité, de leur gravité et de l'importance de la ressource ou de l'identité en question. Au cours de la dernière étape de votre parcours de sécurité (détection avancée), nous allons continuer à nous appuyer sur ces principes en introduisant les alertes basées sur le risque.

Les sources de données qui sont importées, agrégées et structurées dans le framework d'actifs et d'identités sont les suivantes :

- bases de données de gestion de la configuration (CMDB) ;
- outils de découverte des ressources réseau ;
- services d'annuaire et d'authentification ;
- systèmes de ressources humaines ;
- environnements cloud.

Étape 3 : Allez plus loin avec vos données

Le plus souvent, la supervision continue des contrôles de sécurité ne permet pas de détecter les menaces de sécurité avancées. C'est pourquoi la supervision de la sécurité doit examiner le fonctionnement des systèmes cibles, et établir ce qu'est une utilisation autorisée. Il faut également créer une vue globale des systèmes, des données et des utilisateurs, ce qui englobe la supervision des comportements et de l'infrastructure.

Pourquoi ? Parce que l'approche Zero Trust ne peut pas toujours empêcher la fraude, les menaces internes ou les attaques avancées qui se produisent par des moyens autorisés (par exemple, un compte d'utilisateur compromis). Mais une stratégie Zero Trust *peut* contenir un incident et limiter la portée de tout dommage potentiel. Mais si nous ne regardons pas au bon endroit, cependant, il y a fort à parier que ce type de menace ne soit pas détecté à temps. En prenant en compte les politiques Zero Trust et la manière dont un utilisateur autorisé doit se comporter, nous pouvons mieux comprendre les anomalies que nous *devrions* superviser pour mieux détecter les accès malveillants.

Plus de données = moins de stress

En effet, des sources de données supplémentaires, au-delà des simples contrôles de sécurité, doivent être importées pour offrir une meilleure visibilité sur le comportement des utilisateurs. Pour prendre un exemple, il faut extraire les données de flux réseau et mettre en corrélation cette activité avec celle des applications et des processus. On contribue ainsi à détecter les applications non autorisées qui utilisent des communications réseau légitimes et même à identifier les déplacements latéraux entre de multiples applications et comptes d'utilisateur.

Même avec une bonne couverture de supervision grâce aux contrôles et aux politiques régissant l'approche Zero Trust, nous devons toujours prêter une attention particulière à ce que font les utilisateurs et systèmes autorisés une fois l'accès accordé. Aller plus loin que ce que nous disent nos contrôles de sécurité peut nous aider en cas de compromission d'identifiants ou de piratage d'appareils.

Les types de sources de données suivants sont utiles pour détecter ces écarts dans le comportement des utilisateurs et des appareils :

- **Point de terminaison :** comprenez l'exécution des applications et des processus, la supervision de l'intégrité des fichiers et les connexions réseau à l'aide de fonctionnalités étendues de détection et de réponse aux points de terminaison (EDR) ou d'outils tels que sysmon et osquery.
- **Applications :** commencez par les applications stratégiques telles que les systèmes financiers, les systèmes de traitement des données sensibles, les données clients et les logs qui enregistrent les activités des utilisateurs.
- **Base de données :** comprenez les logs d'audit et de transaction afin d'identifier des modèles inhabituels de comportement, la modification ou la suppression d'enregistrements, et les accès non autorisés potentiels à des enregistrements sensibles ou restreints.
- **Cloud :** on s'intéressera principalement aux applications métier SaaS (logiciel en tant que service) pour la supervision des utilisateurs, mais également aux environnements IaaS (infrastructure en tant que service) et PaaS (plateforme en tant que service) afin de détecter les activités administratives suspectes susceptibles de compromettre les stratégies Zero Trust.
- **Services de stockage de fichiers dans le cloud :** il s'agit d'examiner les mouvements de données sensibles pour détecter des modèles inhabituels.

En s'appuyant sur la détection et la supervision initiées à la deuxième étape, nous pouvons enrichir ces scénarios d'utilisation avec des détections plus avancées permises par les sources de données intégrées à la troisième étape. Cela englobe les cas d'utilisation proposés par SSE, mais aussi ceux de Splunk Enterprise Security et des mises à jour de contenu Enterprise Security (ESCU).

Scénarios analytiques

Les scénarios d'utilisation d'ESCU sont des « scénarios analytiques » qui prennent en charge l'ensemble du cycle de vie de l'incident et de la détection, et incluent un récit autour du scénario d'utilisation, des sources de données et des recherches conçues pour faciliter la détection et l'investigation de l'incident.

Exemples de scénarios d'utilisation à la troisième étape :

- déplacement latéral ;
- heure ou emplacement anormal pour l'authentification ou l'accès de l'utilisateur ;
- accès d'un nouvel utilisateur à un ou plusieurs systèmes ou applications ;
- nouveau périphérique de support amovible ;
- création d'un nouveau compte local ;
- utilisation interactive de comptes par défaut, système et de services ;
- processus/applications inhabituels, rares ou jamais vus auparavant ;
- activité inhabituelle en ligne de commande (PowerShell brouillé) ;
- utilisation inhabituelle ou rare d'applications cloud (partage de fichiers) ;
- modifications à un point de terminaison (installation de logiciels, modification de fichiers système).

Étape 4 : Enrichissez et augmentez vos données

Au cours de cette étape, nous allons examiner les sources de données qui fournissent encore plus de contexte : infotmations sur les menaces, informations provenant des outils de gestion des vulnérabilités et des correctifs, et solutions de gestion de la surface d'attaque.

Dresser des remparts contre les menaces

Les informations sur les menaces (TI) nous aident à identifier des indicateurs de compromission (IOC) sur les systèmes protégés et les contrôles Zero Trust. Les utilisateurs peuvent accéder à ces systèmes en temps réel via le framework d'informations sur les menaces de Splunk ES, ou dans le cadre d'un playbook d'enrichissement utilisant les capacités d'automatisation de Splunk SOAR.

Cela nous aide à comprendre le paysage des menaces pour les systèmes et les utilisateurs que nous protégeons, ainsi qu'à identifier les IOC connus qui, autrement, ne seraient pas détectés par des contrôles de sécurité Zero Trust. Par exemple, des adresses IP, des URL et des hashes de fichiers associés à une activité d'hameçonnage, ou les informations d'identification relatives à un certificat SSL connu pour être utilisé à des fins malveillantes.

Deuxièmement, connaître la position des actifs protégés, ainsi que les systèmes utilisés pour accéder à ces ressources, contribue à l'évaluation des risques, à la hiérarchisation des incidents de sécurité, et aux autorisations d'accès. On peut, par exemple, limiter l'accès des systèmes utilisateurs mal sécurisés aux systèmes critiques, et mieux hiérarchiser les incidents de sécurité liés à des vulnérabilités connues.

En outre, les solutions de gestion de la surface d'attaque peuvent vous aider dans la sécurité globale, en concentrant spécifiquement vos efforts sur l'optimisation des contrôles de sécurité et la garantie d'une visibilité de bout en bout. Connaître les lacunes de nos contrôles est un point de départ pour les atténuer ou renforcer la supervision.

En résumé, l'étape d'enrichissement apporte les avantages suivants :

- **Informations sur les menaces en temps réel :** le framework de TI de Splunk Enterprise Security intègre et gère plusieurs flux de TI, commerciaux et open source, et s'appuie sur des protocoles de transport tels que STIX et TAXII. Cette méthode est ensuite utilisée pour reconnaître les IOC entre différentes sources de données Zero Trust, et identifier de manière proactive les menaces connues.

Exemples d'IOC TI types :

  - adresses IP ;
  - FQDN/URL ;
  - noms de fichier et hashes de fichier ;
  - informations de certificat SSL.

- **Supervision du paysage des menaces :** l'infrastructure TI de Splunk Enterprise Security fournit également des fonctionnalités de supervision pour mieux comprendre le paysage des menaces et les tendances spécifiques à votre environnement. La supervision TI examine le taux d'occurrence des différents types de menaces, ainsi que les IOC au sein de votre environnement et des différents flux.
- **Sécurité en temps réel :** Splunk Enterprise Security et le CIM Splunk offrent toute une gamme de fonctionnalités permettant d'acquérir et d'utiliser des données issues de solutions de gestion des vulnérabilités et des correctifs. Ces données peuvent être utilisées pour créer une vue d'ensemble des données de l'entreprise axée sur la sécurité, tout en fournissant du contexte pour la hiérarchisation des incidents de sécurité.

Étape 5 : Automatisation et orchestration avancées

Maintenant que nous avons établi une base solide pour la supervision et les détections de sécurité avec une triple approche (centralisation, normalisation et enrichissement des données) nous pouvons passer à l'enquête et à l'intervention.

Splunk SOAR s'appuie sur l'orchestration et l'automatisation pour rationaliser et accélérer les enquêtes et les mesures correctives en cas d'incident. En utilisant l'automatisation pour contenir et résoudre rapidement les incidents de sécurité grâce à des contrôles de sécurité Zero Trust, Splunk SOAR peut être exécuté via des playbooks avancés ou des requêtes uniques.

Remettez la PEP à votre service

Ces playbooks s'appuient sur une « logique décisionnelle » pour exécuter différentes actions en fonction du contexte de la réponse requise.
Cette fonctionnalité permet à la logique de politique avancée de s'étendre aux capacités de point d'application de stratégie Zero Trust (PEP) et de contrôle d'accès réseau (NAC), en intégrant l'évaluation des risques en temps réel pour perfectionner davantage l'autorisation Zero Trust.

Splunk SOAR peut également définir des procédures d'exploitation standard en conformité avec les cadres industriels tels que NIST 800-61, afin que les analystes puissent suivre le type d'incident qu'ils gèrent à l'aide du manuel ou du modèle de cas correspondant. Cela permet aux analystes de se concentrer sur ce qu'ils font le mieux : interpréter les données.

Le SOAR, une nouvelle vie pour vos données

Tout comme nous avons adopté une approche progressive de l'analyse des données, le SOAR nécessite un traitement similaire :

1. Tout d'abord, identifiez les tâches manuelles et répétitives que les analystes effectuent couramment. C'est là que l'automatisation apportera le plus de valeur.
2. Comprenez et documentez l'ensemble du processus, y compris les différents points de contact technologiques, ainsi que le temps nécessaire à chaque étape. Ce processus peut être documenté à l'aide des manuels Splunk SOAR.
3. Développez un diagramme de flux de processus, en incluant toutes les étapes impliquant des décisions ou des approbations. Cela formera la base du manuel stratégique et de l'automatisation du processus. Identifiez les sections du processus qui peuvent être converties en modules pour être réutilisées comme playbooks secondaires.
4. Identifiez, installez et configurez les applications Splunk SOAR pour prendre en charge l'intégration avec certains composants.
5. Commencez par utiliser le processus défini dans les manuels. Investiguez et répondez aux incidents, et exploitez les capacités présentes via des actions ad hoc.
6. Créez et affinez un playbook pour automatiser progressivement autant de processus que possible, en créant des playbooks modulaires à chaque fois qu'il existe un potentiel de réutilisation.
7. Passez en revue les playbooks et supervisez les performances des analystes au fil du temps pour comprendre ce qui fonctionne. Recherchez d'autres possibilités d'amélioration.

Voici quelques exemples de scénarios d'utilisation Zero Trust pour Splunk SOAR :

- Manuels/modèles de cas définissant la prise en charge et l'exploration des incidents Zero Trust. Quelques exemples :
  - compromission de compte ;
  - violation des données.
- Playbooks permettant d'automatiser la réponse aux incidents Zero Trust. Quelques exemples :
  - réinitialisation de mot de passe ou verrouillage de compte dans Active Directory ;
  - confinement d'e-mail compromis et réponse ;
  - investigation et prise en charge d'hameçonnage par e-mail ;
  - confinement des appareils perdus/volés ;
  - confinement des acteurs malveillants internes ;
  - confinement des programmes malveillants et réponse ;
  - confinement des ressources web malveillantes et réponse.

Et ce n'est pas tout. Les analystes n'ont plus besoin de se connecter directement aux contrôles Zero Trust. Splunk SOAR s'intègre aux solutions de gestion des accès privilégiés (PAM), ce qui permet à l'utilisateur d'effectuer des actions directement depuis l'application.

Il est également possible de mettre en œuvre un niveau d'autorisation avancé au-delà des solutions PEP/NAC Zero Trust. Maintenant, en examinant la posture de risque et son évaluation en temps réel, nous pouvons nous appuyer sur des informations plus nombreuses encore pour autoriser l'accès des utilisateurs, ce qui nous permet d'enrichir les politiques traditionnelles d'accès et d'autorisation Zero Trust. On peut ainsi combiner et évaluer les scores de risque de l'utilisateur *et* du système auquel il tente d'accéder, pour mieux comprendre le profil de risque de ce point de terminaison.

Automatisez les tâches SOC manuelles

Pendant (et même après) la phase d'autorisation, Splunk SOAR peut être utilisé pour évaluer le profil de risque des actifs et des identités dans Splunk ES, et déterminer si un accès doit être accordé ou révoqué, en plus de toute autre action à entreprendre. Le résultat peut ensuite être partagé avec le NAC ou le moteur de stratégie Zero Trust et utilisé pour autoriser, refuser ou révoquer un accès. En cas de refus d'accès, Splunk SOAR peut prendre des mesures supplémentaires, selon les raisons du refus.

Quelques exemples :

- refuser l'accès utilisateur et émettre une notification en raison d'un score de risque élevé ;
- limiter l'accès de l'utilisateur si un comportement inhabituel ou risqué est observé après l'autorisation initiale ;
- lancer des analyses de vulnérabilité du système ou d'inventaire sur les actifs qui montrent des signes de comportement inhabituel après autorisation ;
- créer automatiquement des tickets d'assistance IT pour les systèmes non conformes auxquels un accès a été refusé ;
- lancer automatiquement les activités de correction telles que l'application de correctifs, la désactivation de logiciels/services non autorisés ou la (ré)application de contrôles de sécurité.

Étape 6 : Détection des menaces avancées

Nous en sommes enfin à la dernière étape de l'implémentation d'une architecture Zero Trust. Nous allons maintenant définir des détections de sécurité avancées avec des alertes basées sur le risque (RBA). Cela vous permettra de garantir la fidélité des menaces de votre file d'attente et de réduire le volume global d'alertes. Nous pouvons également commencer à élargir les capacités de Splunk Enterprise Security avec Splunk UEBA.

L'objectif ici est de réfléchir aux points suivants : **1.** Les politiques entourant l'approche Zero Trust, **2.** Ce que les utilisateurs font généralement avec les systèmes auxquels ils ont accès, et **3.** Comment identifier des modèles de comportement qui pourraient être révélateurs d'une activité inhabituelle ou malveillante.

Tout d'abord, vous devrez vous appuyer sur les scénarios de détection antérieurs : vous pourrez ainsi examiner les différentes phases d'un incident de sécurité (la « kill chain ») et commencer à utiliser plusieurs indications d'activité suspecte pour générer une alerte.

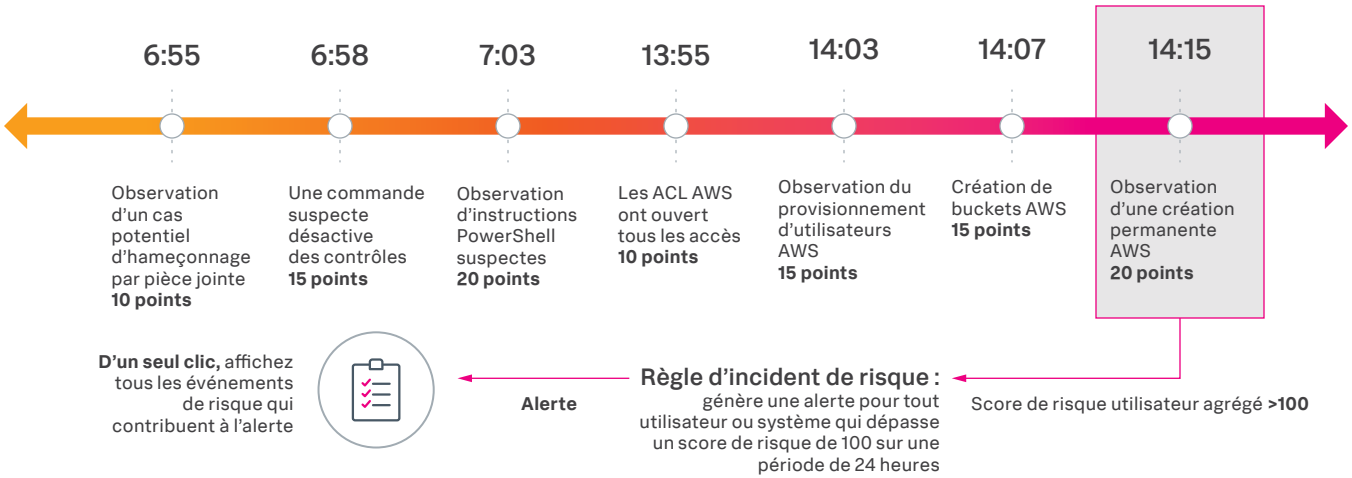
Sauvez le monde avec RBA

Selon le principe d'alerte basée sur le risque, au lieu de générer une alerte au premier signe d'une menace potentielle, on crée simplement un enregistrement de l'événement. Une fois cet événement consigné, toute autre indication d'activité malveillante sera signalée. De cette façon, nous pouvons désormais voir la séquence ou le schéma des événements par rapport à l'actif ou à l'identité en question, soigneusement encapsulés dans une seule alerte.

Dans l'exemple suivant, nous voyons comment l'exfiltration des données a été précédée d'un certain nombre d'événements inhabituels. Avant le RBA, chaque événement générait une alerte unique, qui avait toutes les chances de se perdre dans la masse. Mais en observant toute la kill chain et en utilisant plusieurs indicateurs, nous pouvons générer une alerte unique avec un niveau de confiance plus élevé.

Alerte basée sur le risque dans une optique Zero Trust

Plusieurs événements liés à la stratégie Zero Trust deviennent un contexte qui informe les alertes haute fidélité



Nous pouvons également introduire des fonctionnalités d'évaluation des risques plus avancées, qui approfondissent la façon dont les alertes sont hiérarchisées. Par exemple, le cadre standard d'évaluation des risques de Splunk ES examine l'importance de l'actif ou de l'identité, ainsi que la gravité de l'alerte, pour déterminer l'évaluation de risque dynamique.

Avec RBA, nous pouvons inclure des dimensions supplémentaires qui soutiennent le modèle Zero Trust. Voici quelques exemples de scénarios d'utilisation utiles :

- techniques couvrant plusieurs tactiques MITRE Zero Trust sur une période de 24 heures ;
- plusieurs techniques MITRE Zero Trust associées à une même tactique sur une période de 24 heures.

Même si RBA et UEBA fonctionnent différemment, ils ont en commun d'utiliser plusieurs indicateurs pour identifier les activités suspectes ou malveillantes. Grâce aux nombreux points de référence sur lesquels ces outils s'appuient, ils sont mieux placés pour générer des alertes de fidélité plus élevées tout en réduisant le nombre de faux positifs.

Analyse du comportement des utilisateurs et des entités

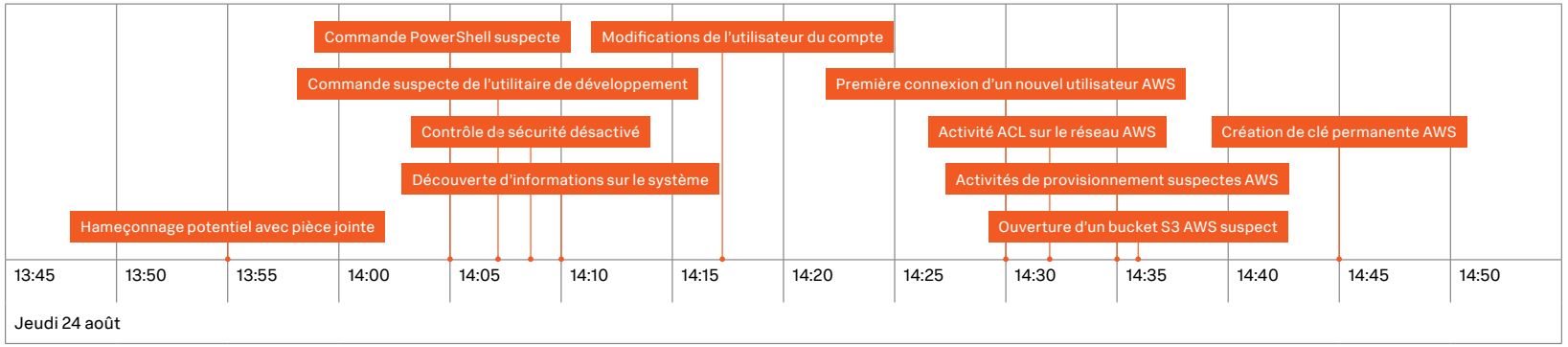
Le machine learning non supervisé de Splunk UEBA nous aide à rechercher les anomalies dans l'activité des utilisateurs, des appareils et des applications. Dans de nombreux cas, ces événements sont inoffensifs (même inhabituels). Mais, en utilisant une approche similaire au RBA, l'UEBA recherche des modèles et des séquences qui se rapportent aux différentes étapes d'un incident de sécurité et regroupe automatiquement ces événements anormaux en une seule alerte ou menace.

Comme avec le RBA, on augmente ainsi la fiabilité de l'alerte, tout en allégeant les efforts des analystes en lien avec l'identification manuelle des événements connexes. Au-delà de l'analyse comportementale, les capacités fournies par Splunk UEBA apportent également un contexte plus riche et associent l'activité des utilisateurs aux systèmes et données auxquels ils accèdent.

Voici quelques exemples d'approche comportementale du modèle Zero Trust (qui s'applique aux menaces internes et avancées) :

- exfiltration des données par un compte utilisateur compromis ;
- exfiltration des données par un acteur interne ou un utilisateur à risque de fuite ;
- détection des mouvements latéraux avancés ;
- escalade des privilèges avancés.

Affichage de la chronologie des menaces Zero Trust avec RBA



Le modèle Zero Trust requiert une approche écosystémique

La mise en place d'une politique Zero Trust complète implique une gamme de composants intégrés. Ensemble, ces contrôles fournissent les données et les informations nécessaires pour une supervision centralisée.

En alignant les méthodologies Zero Trust sur l'écosystème de partenaires de Splunk, nous pouvons améliorer considérablement la sécurité des entreprises et leurs opérations de sécurité globales.

Lisez les pages suivantes pour découvrir les capacités de nos partenaires Zero Trust et comment ils peuvent vous aider à atteindre vos objectifs Zero Trust.

Zscaler

Zscaler, l'un de nos principaux partenaires stratégiques, est un fournisseur de sécurité et un innovateur de premier plan qui connecte les utilisateurs à Internet en toute sécurité, ainsi qu'à une multitude d'applications privées. Zero Trust Exchange de Zscaler est une architecture proxy native du cloud qui connecte directement les utilisateurs et les applications aux ressources de l'entreprise, sans créer d'exposition supplémentaire inutile. Zscaler renforce cette architecture par une inspection SSL (Security Sockets Layer), une authentification forte et de riches contrôles basés sur des politiques.

Voici deux de leurs principales solutions Zero Trust :

Zscaler Internet Access (ZIA) offre une sécurité complète aux utilisateurs qui se connectent à Internet, où qu'ils se trouvent. Le service de Zscaler est assuré par 150 datacenters dans le monde entier, ce qui permet aux utilisateurs de bénéficier d'une expérience rapide, sécurisée et sans complication.

Zscaler Private Access (ZPA) favorise un accès transparent et basé sur le moindre privilège aux applications traditionnelles et cloud pour les utilisateurs locaux et distants, en éliminant la complexité des solutions traditionnelles de segmentation de réseau et d'accès à distance. La surface d'attaque des applications est considérablement réduite car elles sont invisibles aux canaux publics.

Splunk intègre la télémétrie haute fidélité de Zscaler avec une intégration prête à l'emploi du cloud au cloud, offrant aux équipes de sécurité une visibilité sur leur trafic cloud et réseau, et les aidant à détecter et à éliminer les menaces émergentes dans toute l'entreprise. L'API Zscaler permet également aux analystes de sécurité de mener des actions coordonnées sur la plateforme Zscaler et d'autres outils de sécurité à l'aide de Splunk SOAR, en orchestrant l'accès des utilisateurs et la gestion des politiques via un module complémentaire d'application et de technologie disponible sur Splunkbase.

Systèmes DTEX

DTEX,première et seule plateforme mondiale de cyber-intelligence sur la main-d'œuvre, capture la télémétrie comportementale de tous les points de terminaison, produisant des « indicateurs d'intention » dynamiques et une connaissance en temps réel des activités se déroulant au sein de l'entreprise, sans pour autant enfreindre la protection de la vie privée.

Grâce à des structures d'évaluation complexes, DTEX peut vous aider à voir, comprendre et exploiter l'intelligence contextuelle, et à améliorer la capacité de votre entreprise à arrêter les menaces internes, prévenir la perte de données, optimiser les investissements logiciels et protéger votre personnel. Ce niveau de visibilité est essentiel pour une détection avancée des menaces internes et externes, et il constitue une source étendue de données pour la détection des anomalies comportementales.

Pour une meilleure mise en œuvre des détections de sécurité avancées Zero Trust et des scénarios d'utilisation de la supervision, consultez l'intégration DTEX-Splunk sur Splunkbase, disponible en tant qu'extension d'application.

CloudKnox

En raison de la multiplication des identités et des politiques dans les services natifs du cloud, il devient de plus en plus difficile de gérer et de sécuriser les différents types d'utilisateurs et leur niveau d'accès. Il existe aujourd'hui un fossé considérable entre les autorisations accordées et les autorisations utilisées : la plupart des identités utilisent moins de 5 % des autorisations à haut risque. De ce fait, il est devenu beaucoup plus difficile d'appliquer des stratégies de moindre privilège, ce qui expose les entreprises à des risques élevés et les empêche de gérer correctement les accès Zero Trust.

Ce qui nous amène à CloudKnox, une plateforme de gestion et de supervision des autorisations multicloud/cloud hybride qui protège les ressources et les identités de l'infrastructure cloud stratégique en fournissant une visibilité complète, une correction automatisée et une supervision continue des autorisations. Grâce à la technologie « Activity Based Authorization », brevetée par CloudKnox, la plateforme CloudKnox permet aux entreprises de mettre en œuvre des stratégies Zero Trust sur tous les clouds avec un modèle d'exploitation unique. CloudKnox prend en charge VMware vSphere (à la fois sur site et dans le cloud), AWS, Azure et GCP.

CloudKnox est un partenaire de sécurité stratégique de Splunk pour l'approche Zero Trust, et la plateforme est prise en charge par une extension Splunkbase. La plateforme de gestion des autorisations CloudKnox a été déployée et intégrée à Splunk dans de nombreuses entreprises du monde entier, parmi lesquelles beaucoup de membres du Fortune 500.

Okta

Okta est une plateforme cloud-native de confiance pour sécuriser chaque identité, des clients aux employés. Plus de 10 000 entreprises font confiance aux solutions d'identités d'Okta pour connecter, autoriser et gérer l'accès des utilisateurs aux applications et données critiques sur leurs architectures hybrides, prenant ainsi en charge un aspect clé d'une approche globale Zero Trust. Les données d'authentification et d'autorisation, ainsi que le contexte des identités d'Okta, fournissent une source d'informations riche pour prendre en charge les exigences de supervision de sécurité Zero Trust avec l'approche Splunk. Grâce à l'intégration avec Splunk, fournie par l'extension Okta disponible sur Splunkbase, les clients peuvent rapidement intégrer et utiliser leurs données pour atteindre des objectifs Zero Trust.

Ilumio

Grâce à une approche leader sur le marché, Ilumio a transformé la sécurité en aidant les entreprises à cartographier leurs applications, leur connectivité, leurs points de terminaison et leurs applicatifs, et en mettant en œuvre une micro-segmentation Zero Trust, de sorte que seules des communications fiables puissent se produire dans les environnements cloud, hybrides, multicloud et locaux. Découvrez les nombreuses fonctionnalités Zero Trust d'Ilumio, comme la télémétrie complète de sécurité du réseau, en téléchargeant l'application Ilumio disponible sur Splunkbase. L'application offre des fonctionnalités avancées de supervision et de reporting pour soutenir les équipes IT, de sécurité et de conformité. Elle offre également une meilleure visibilité sur le trafic des applications dans Splunk, ce qui vous permet de mettre rapidement en quarantaine les applicatifs suspects d'un simple clic.

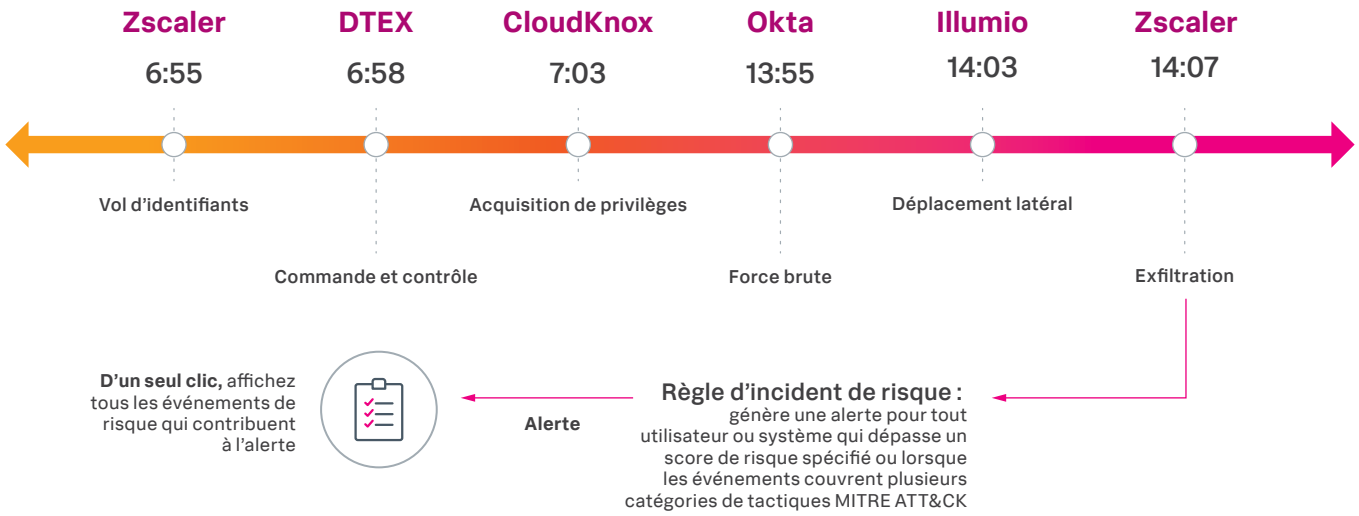
Votre écosystème Zero Trust en action : un exemple

Si nous examinons les catégories MITRE ATT&CK que nous avons définies, outre les nombreuses étapes que nous avons identifiées dans le cadre de votre parcours de sécurité, nous pouvons voir comment les technologies Zero Trust détaillées précédemment prennent en charge chaque scénario d'utilisation. Le diagramme suivant fournit un exemple pratique de ce que permet cette approche commune. Chacune de ces solutions partenaires offre une couverture étendue pour assurer la détection de ces tactiques MITRE ATT&CK liées à l'approche Zero Trust, et peut être combinée à d'autres sources de données pour une meilleure visibilité.

- **Accès initial :** Zscaler Private Access fournit la télémétrie nécessaire pour détecter un accès suspect ou anormal à des applications protégées, pouvant indiquer que des informations d'identification valides ont pu être volées ou piratées.
- **Persistance :** les données granulaires de points de terminaison fournies par DTEX permettent de détecter les techniques imparables utilisées par les attaquants qui tentent d'établir une présence via des techniques de commande et de contrôle.
- **Acquisition de privilèges :** grâce aux fonctionnalités de supervision avancées fournies par CloudKnox, nous pouvons détecter les modifications apportées aux privilèges d'administrateur ou de développeur dans les environnements cloud hybrides, telles que l'utilisation anormale d'identifiants d'administration cloud valides.
- **Accès aux identifiants :** Okta fournit des données d'authentification et d'autorisation détaillées qui permettent à Splunk de détecter une activité anormale, signe potentiel d'accès suspect aux identifiants, comme dans le cas d'attaques par force brute.
- **Déplacement latéral :** grâce à l'approche de microsegmentation d'Illumio, qui offre une visibilité granulaire sur l'activité du réseau dans les environnements hybrides, nous sommes en mesure de détecter les techniques de déplacement latéral, réussies ou non.
- **Exfiltration :** Zscaler Internet Access prend en charge la supervision de l'activité web pour permettre la détection d'anomalies avec Splunk, afin d'identifier l'exfiltration potentielle de données sur une large gamme de services web.

Examen de tout le spectre de tactiques MITRE ATT&CK

Alertes multi-sources, multi-indicateurs, haute fidélité pour l'approche Zero Trust avec RBA

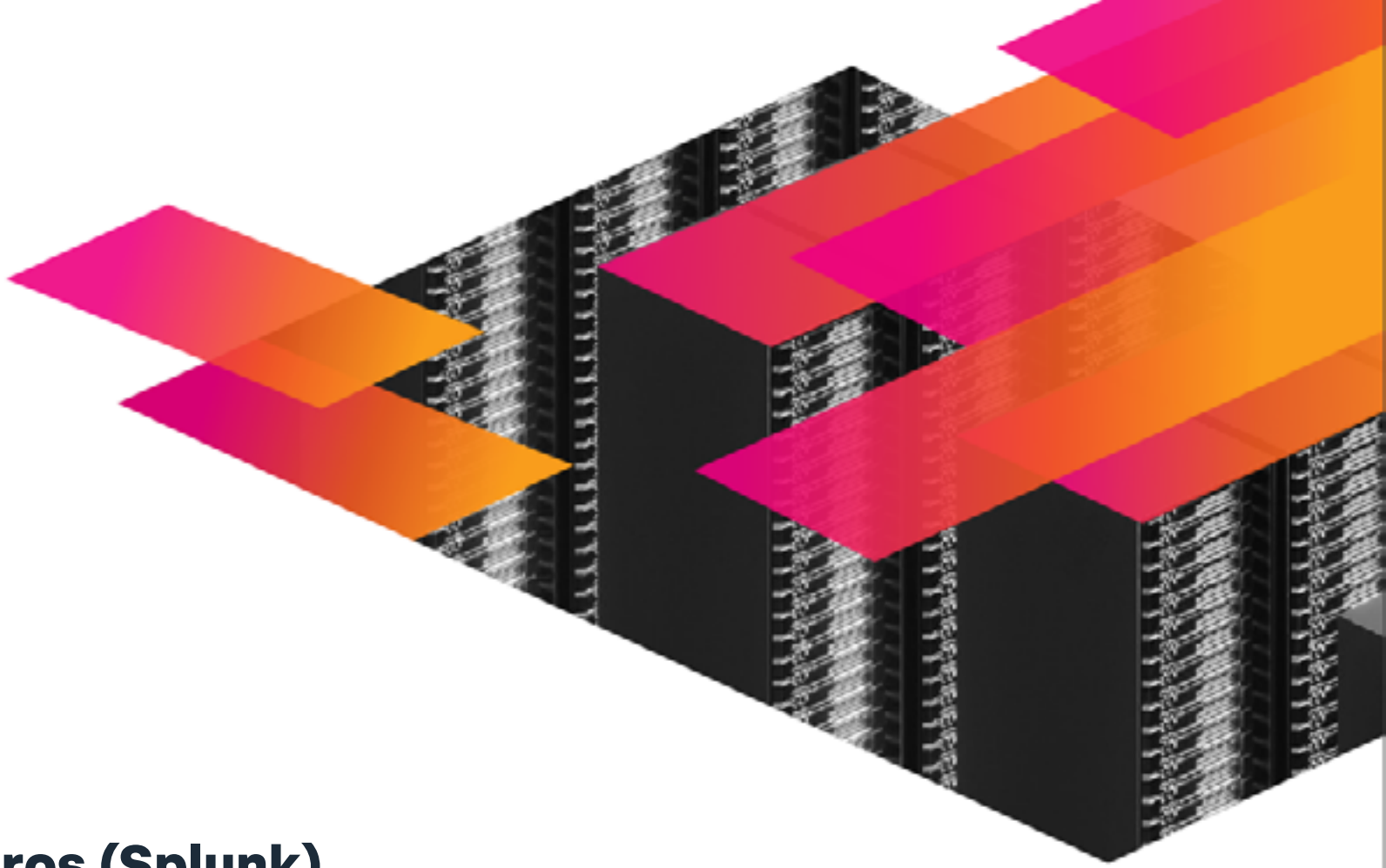


Une approche Zero Trust axée sur les données

Nous atteignons la fin de votre voyage vers l'approche Zero Trust. Il faut garder en tête que l'approche de sécurité axée sur les données présente d'innombrables avantages, en particulier lorsqu'il s'agit de mettre sur pied une architecture Zero Trust.

Les données sont au centre de toute stratégie réussie, notamment en matière de *sécurité*. Mais trop souvent, les systèmes et les structures dont nous dépendons finissent par piéger ou segmenter nos données, ce qui rend beaucoup plus difficile l'extraction de leur immense valeur.

La bonne nouvelle ? Vous pouvez supprimer ces obstacles et libérer une mine d'informations et d'opportunités grâce à l'analyse des données, tout en bénéficiant d'une réelle compréhension de la politique Zero Trust, des rôles et des ressources de votre entreprise. Grâce à la flexibilité et à l'ouverture du portefeuille Splunk, les équipes peuvent désormais connecter des technologies disparates et appliquer des mesures ciblées, prendre de meilleures décisions, plus rapides et plus efficaces à l'échelle de l'entreprise, et, en fin de compte, adopter une robuste stratégie Zero Trust.



De zéro à héros (Splunk)

Quel que soit votre avancement sur le parcours Zero Trust, Splunk peut vous aider à garder une longueur d'avance sur les menaces nouvelles et actuelles. Découvrez comment moderniser vos opérations de sécurité et renforcer la sécurité de votre entreprise en téléchargeant Splunk Security Essentials dès aujourd'hui.

21-18251-Splunk-The Essential Guide to Zero Trust-EB-109

splunk> turn data into doing™