Le guide fondamental

pour construire

un meilleur SOC

splunk>

turn data into doing™

Il est difficile d'anticiper les cybermenaces. La détection des menaces inconnues ou cachées est encore plus compliquée, en particulier lorsque les outils de sécurité existants et hérités ne tiennent pas compte de la complexité et du volume des menaces avancées de sécurité.

Ces solutions obsolètes ne parviennent pas à détecter les risques posés par les menaces internes, les malwares à déplacement latéral et les comptes compromis, en partie parce qu'elles n'ont pas été conçues pour affronter les cybermenaces d'aujourd'hui, mais aussi parce que les solutions logicielles sur lesquelles reposent les centres d'opérations de sécurité (SOC) inondent les analystes d'un volume considérable d'alertes qui sont en grande partie erronées.

Même si votre équipe travaille dur et a beaucoup de talent, il y aura toujours un arriéré considérable d'incidents de sécurité - et cela ne va pas aller en s'améliorant. En réalité, il n'y a tout simplement pas assez de professionnels qualifiés dans le domaine de la sécurité - à vrai dire, il en manque 3,5 millions - et ceux qui existent coûtent cher.

En fait, leur travail devient plus difficile à cause des outils qu'ils utilisent. Les outils obsolètes utilisés dans le SOC d'aujourd'hui absorbent les budgets. Par ailleurs, ils sont conçus par différents fournisseurs qui ne fonctionnent pas bien ensemble. Lorsque les fournisseurs ne s'intègrent pas bien, les processus sont ralentis et les données sont perdues.

Par conséquent, les analystes ne peuvent souvent pas voir tout ce qu'il se passe dans l'entreprise. En effet, les décideurs commerciaux et informatiques estiment qu'en moyenne 55 % de leurs données sont des dark data, inconnues ou inexploitées. Comment les professionnels de la sécurité sont-ils censés sécuriser ce qu'ils ne peuvent pas voir alors que la plupart des données disponibles ne sont pas visibles ? Après tout, toutes les données sont importantes en matière de sécurité.

La compréhension des origines d'un SOC est donc impérative pour donner un sens aux problèmes d'aujourd'hui. Les SOC sont initialement apparus comme le nouveau centre de gravité des opérations de sécurité, tant physiques que virtuelles. Ils nécessitent un entretien constant, une expansion et une rapidité sans précédent pour en tirer profit.

Le quotidien des analystes SOC s'est rapidement axé sur le triage et le suivi des alertes. Les analystes de niveau 1 ont été rapidement dépassés face au trop grand nombre d'alertes à gérer, noyés dans le sentiment de toujours prendre du retard.

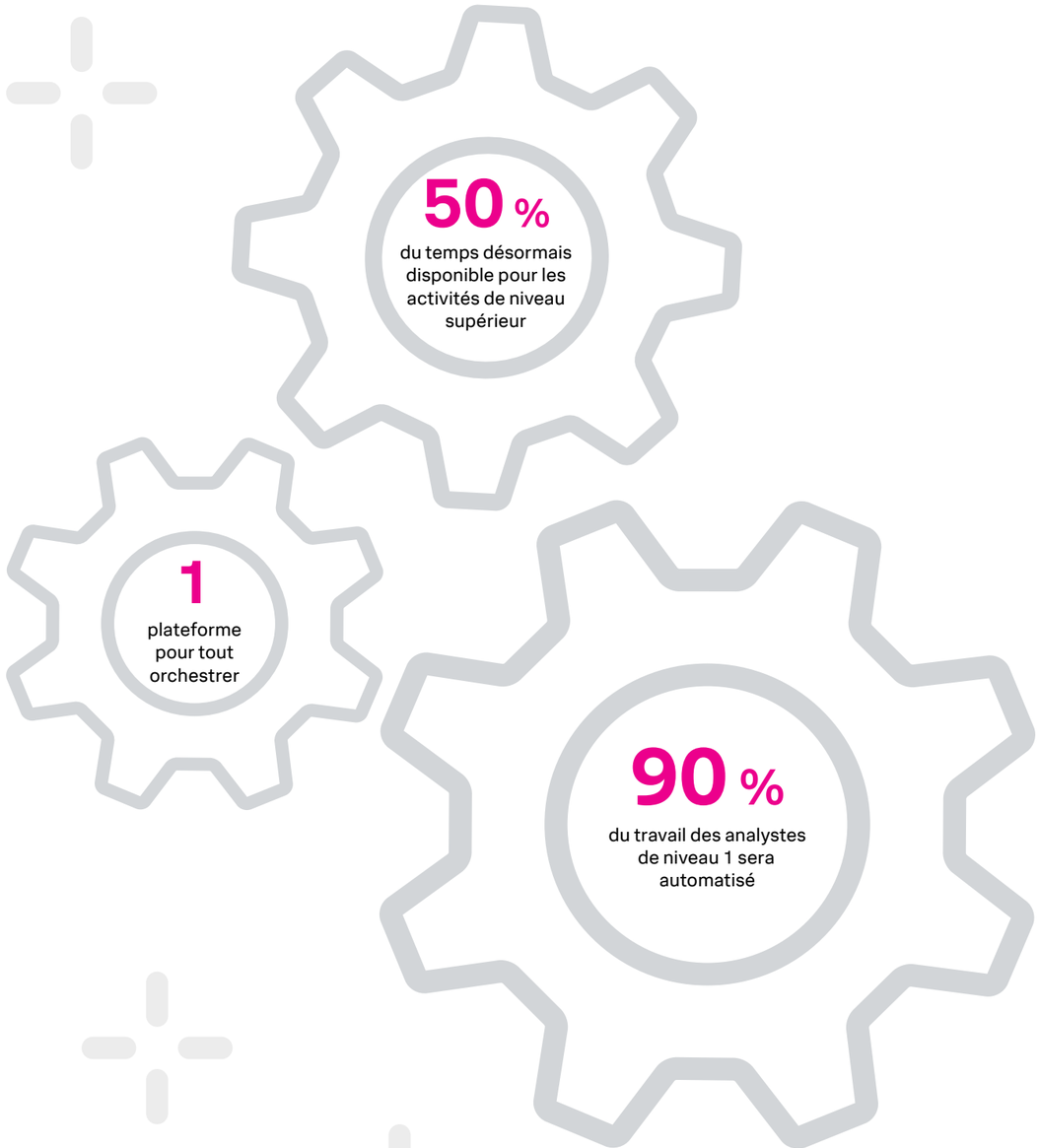
Leur travail a été rendu plus difficile car 80 % des SOC ont été construits sur des systèmes disparates et déconnectés.

Nous devons tous intégrer cette nouvelle réalité : Il n'y a tout simplement pas assez de professionnels qualifiés pour analyser le volume d'incidents auxquels les analystes sont confrontés, et la plupart ne disposent pas des bons outils pour combler les lacunes.

Dans ce contexte, que doivent faire les entreprises qui utilisent des technologies antédiluviennes ? À moins de cloner tous leurs analystes SOC et de trouver une mine d'or pour les payer, tout repose sur la technologie que les entreprises utilisent pour permettre à leurs analystes d'anticiper les menaces.

Les équipes de sécurité doivent répondre aux nouvelles menaces en ajoutant de nouvelles capacités analytiques à leur SOC, ce qui leur donne plus d'informations sur les menaces potentielles avant qu'elles ne deviennent de gros cyber-monstres effrayants. Elles ont besoin d'outils qui permettent aux professionnels de la sécurité d'automatiser certains processus afin de pouvoir se concentrer sur les alertes réelles, autrement dit, les menaces réelles.

Il est temps de construire un meilleur SOC.
Il est temps de construire la prochaine génération de SOC.



Construire le SOC du futur aujourd'hui

À l'avenir, 90 % du travail des analystes de niveau 1 sera automatisé. La majeure partie de leur charge de travail est banale et répétitive. L'automatisation permet aux analystes de se concentrer sur ce qui compte vraiment.

Ensuite, nous nous attendons à ce que le temps passé à trier les alertes soit désormais consacré à ajuster la logique de détection et de réponse, notamment en créant des règles de corrélation et des procédures pour accroître l'automatisation. Nous estimons que 50 % du temps d'un analyste sera consacré à des activités de valeur supérieure.

Enfin, nous espérons que des plateformes comme Splunk se connectent et créent une plateforme unique pour superviser et investiguer les événements, ce qui éliminerait la nécessité de naviguer entre des dizaines de produits.

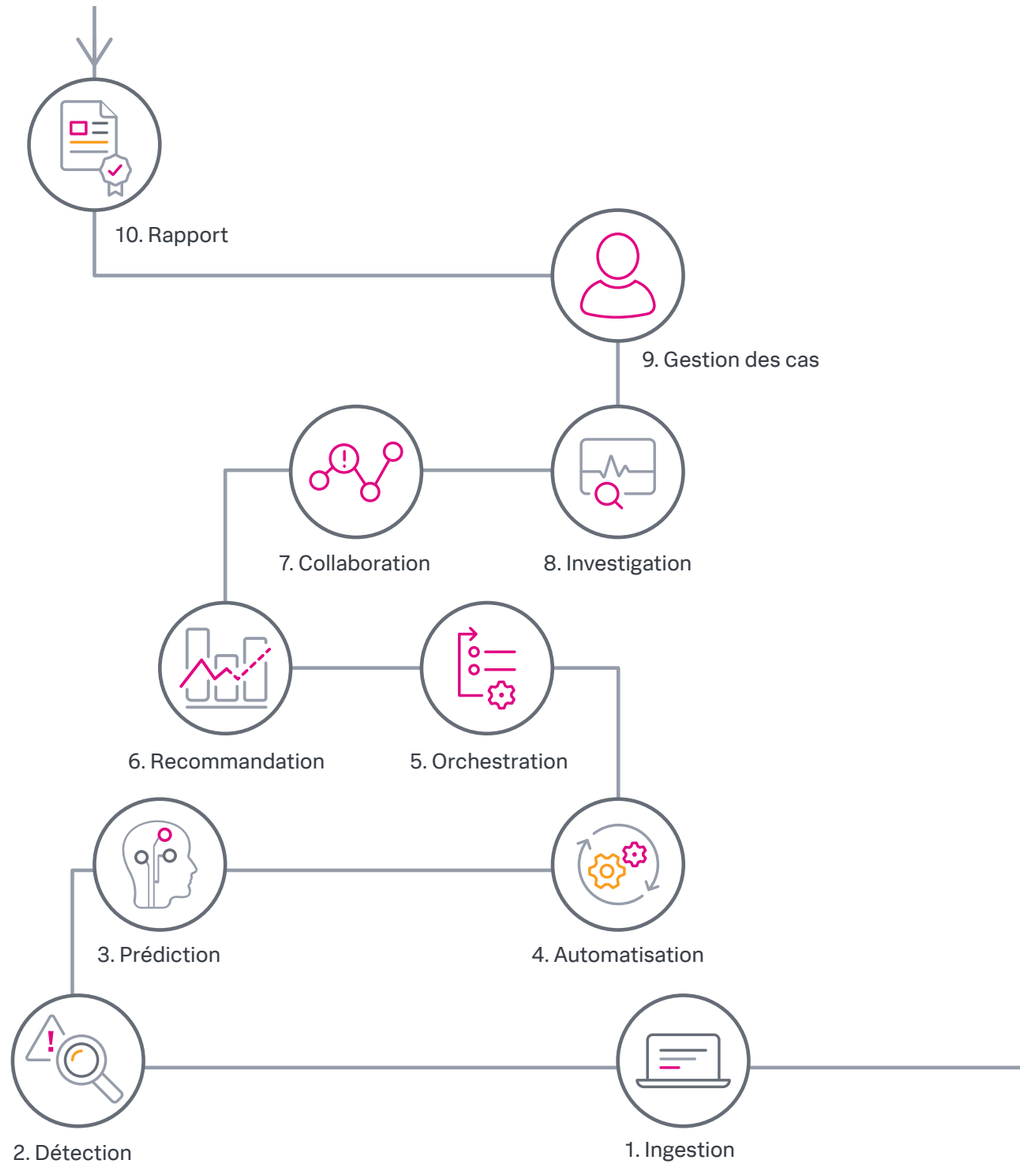
Les organisations ne doivent pas attendre demain pour obtenir la **technologie dont elles ont besoin aujourd'hui.**

En fait, la construction d'un SOC du futur commence réellement par l'adoption d'un état d'esprit selon lequel il est normal d'alimenter un SOC avec une plateforme délibérément construite, puis de brancher les outils d'automatisation et de machine learning nécessaires. Tout est une question d'adoption de l'approche selon laquelle il est acceptable de devenir le patron du SOC.

Le SOC de nouvelle génération est construit sur une suite unique qui intègre de façon transparente les solutions d'autres fournisseurs pour augmenter les capacités existantes. Il ne s'agit pas d'une solution qui est reconstituée ad hoc.

La suite de sécurité doit également disposer de puissantes fonctionnalités d'analyse qui peuvent optimiser les capacités d'une petite équipe, leur donnant un aperçu des menaces potentielles pour leur éviter de perdre du temps sur de fausses alertes. Enfin, la suite peut exploiter les technologies avancées de machine learning (ML), d'automatisation et d'orchestration.

Plus précisément, pour construire le SOC du futur aujourd'hui, les organisations ont besoin d'une plateforme d'opérations de sécurité qui prend en charge 10 capacités :



1. Ingestion

Tout commence par les données. Les données sont l'oxygène qui donne vie à un SOC. Les analyses et les algorithmes le respirent. La capacité d'ingérer des données à grande échelle à partir de n'importe quelle source, structurée ou non structurée, est tout aussi importante. Vous devez également pouvoir organiser ces données pour les rendre utilisables par la machine ou par l'homme.

2. Détection

Une fois qu'un événement est entré dans le système, il est impératif que la suite d'opérations de sécurité puisse détecter l'événement. Dans ce cas, la détection se concentre sur les événements, ce qui diffère des solutions traditionnelles qui se focalisaient sur les fichiers ou le trafic réseau. Une suite d'opérations de sécurité peut exploiter une combinaison de règles de corrélation, de machine learning et de scénarios analytiques, pour n'en nommer que quelques-unes.

3. Prédiction

Imaginez que vous recevez une alerte 30 minutes avant de découvrir un événement de sécurité. Imaginez ce que cela représenterait pour votre SOC. La capacité de prédire un événement de sécurité permet au SOC de transmettre de manière proactive l'incident à un être humain ou de rationnaliser une réponse grâce à un processus prédéfini. Il existe de nouvelles technologies prédictives très prometteuses qui fournissent aux analystes une alerte précoce, des précurseurs ou des indicateurs d'attaques plus importantes, et qui identifient les menaces inconnues avant qu'elles ne deviennent des risques plus importants.

4. Automatisation

L'automatisation est l'une des technologies les plus récentes au service des analystes SOC. L'acquisition de Phantom par Splunk en est un excellent exemple. Les outils d'automatisation transforment des procédures d'exploitation standard en guides opérationnels numériques pour accélérer l'investigation, l'enrichissement, la détection, l'isolation et la correction.

Un SOC doté de capacités d'automatisation peut traiter davantage d'événements car les processus qui prenaient par exemple 30 minutes peuvent désormais être effectués en 40 secondes seulement. Dans l'évolution d'un SOC, l'automatisation n'est plus un choix mais bien un outil obligatoire.

5. Orchestration

Vous avez acheté des dizaines de produits pour faire fonctionner votre SOC par nécessité, non pas parce que vous aviez un budget supplémentaire. La majorité de ces outils ont leur utilité et renforcent votre défense, mais ils ne changeront probablement pas. Cette situation est problématique car les menaces évoluent et les produits qui détectent les menaces doivent suivre le rythme dans un monde axé sur les API. C'est là que l'orchestration entre en jeu. L'orchestration vous permet de brancher et de connecter tout ce qui se trouve à l'intérieur et à l'extérieur de votre SOC. Vous ne devez plus ouvrir de nouveaux onglets de navigateur pour chaque produit et vous éliminez le copier-coller de plusieurs solutions. La possibilité d'orchestrer tous vos produits supprime les frais généraux, réduit la frustration et aide les analystes à concentrer leur énergie sur des tâches utiles.

6. Recommandation

À ce stade, les événements ont transité par une machine. Imaginez que la plateforme qui alimente le SOC puisse indiquer aux analystes les actions qu'ils doivent prendre. Le SOC de nouvelle génération peut faire exactement cela en formulant une recommandation. Cela peut prendre la forme d'actions individuelles ou de procédures. Les recommandations sont utiles de deux manières : 1) elles instruisent les nouveaux analystes et leur apprennent ce qu'ils doivent faire lorsqu'une menace similaire se présente à nouveau, et 2) elles servent de vérification aux analystes expérimentés, ou de rappel d'un accélérateur pour les assister dans ce qu'ils devraient déjà savoir.

7. Investigation

Comme nous l'avons mentionné plus haut, nous nous attendons à ce que 90 % du travail des analystes de niveau 1 soit automatisé dans un avenir proche. Qu'advient-il du reste du travail ? Inévitablement, une analyse humaine détaillée et précise est nécessaire pour terminer le travail. Des outils de sécurité intuitifs assistent la capacité humaine d'un analyste et lui permettent de donner la priorité à ce qui doit vraiment être investigué.

8. Collaboration

La sécurité est un sport d'équipe qui nécessite une coordination et une communication. En d'autres termes, cela exige une collaboration. Dans un environnement SOC, rien ne peut être abandonné. Les événements doivent être traités dans les moindres détails et les équipes doivent avoir des fonctionnalités ChatOps ou la capacité de collaborer et de connecter les outils, les personnes, les processus et l'automatisation dans un lieu de travail transparent. Les informations, les idées et les données sont mises au premier plan. Cela permet aux équipes de sécurité de mieux collaborer, d'inviter des personnes extérieures au SOC à participer aux alertes, de partager des informations urgentes et importantes avec des pairs, et enfin de coopérer en tant qu'industrie.

9. Gestion des cas

Des incidents se produisent même lorsque nous faisons de notre mieux pour les éviter. L'important, c'est que lorsque des incidents surviennent, les équipes de sécurité soient munies de tous les outils nécessaires pour gérer le processus de réponse. Les équipes doivent s'assurer de disposer de plan de réponse, de workflows, de collecte de preuves, de communication, de documentation et de chronologies. La gestion des cas est donc devenue une capacité de base du SOC de nouvelle génération.

10. Rapport

On ne peut pas gérer ce qu'on ne mesure pas. Nous vivons dans un monde piloté par les données et il en va de même pour la sécurité. C'est pourquoi vous pouvez désormais mesurer tous les aspects du processus de sécurité. Le fait de disposer des bons outils d'établissement de rapports fournit des renseignements sur ce qui fonctionne. Ainsi, les équipes de sécurité peuvent mesurer avec précision où elles se trouvent et où elles doivent aller. Aujourd'hui, le défi auquel les SOC sont confrontés est leur dépendance à un nombre trop élevé de plateformes, ce qui rend impossible l'obtention de rapports précis.

Splunk entre en jeu

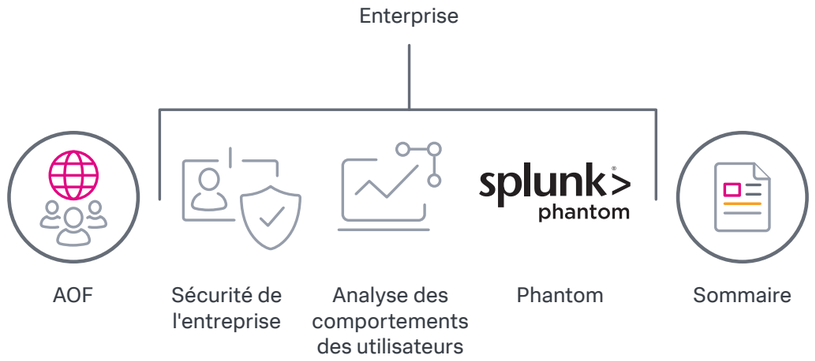
La suite Splunk pour les Opérations de sécurité réunit les meilleures technologies SIEM, UEBA et SOAR au sein d'une même plateforme pour faire fonctionner le SOC de prochaine génération. Aucun concurrent de Splunk ne peut prétendre avoir toutes les solutions dans une seule plateforme.

Splunk prend non seulement en charge ces capacités, mais aussi les cas d'utilisation suivants :

Supervision en temps réel	Splunk Enterprise, Splunk Cloud ou Splunk Enterprise Security
Investigation	Splunk Enterprise, Splunk Cloud ou Splunk Enterprise Security
Automatisation et orchestration	Splunk Phantom
Détection des menaces avancées et internes	Splunk User Behavior Analytics ou Splunk Enterprise Security
Réponse aux incidents	Splunk Phantom ou Splunk Enterprise Security
Conformité	Splunk Enterprise, Splunk Cloud ou Splunk Enterprise Security

La plateforme Splunk, aussi connue sous le nom de Splunk Cloud ou Splunk Enterprise, est votre point de départ. C'est ici que vous ingérez vos données. Splunk est une plateforme personnalisable d'analyse de données qui transforme les données machine en résultats commerciaux tangibles. Contrairement au SaaS et aux autres alternatives open source, Splunk Cloud et Splunk Enterprise vous permettent d'exploiter vos investissements technologiques existants. Vous pouvez tirer parti de toutes les données générées par vos systèmes, applications et appareils informatiques, de sécurité et d'entreprise, pour investiguer, superviser, analyser et agir en temps quasi réel.

La suite Splunk pour les **Opérations de sécurité**



Plus précisément, la suite Splunk pour les Opérations de sécurité se compose de :

Splunk Enterprise Security (ES) est une solution SIEM axée sur l'analyse qui fournit une supervision de la sécurité en temps réel, une détection avancée des menaces, une investigation et un examen des incidents, ainsi qu'une réponse aux incidents pour une gestion efficace des menaces.

Grâce à **Splunk ES**, les équipes de sécurité bénéficient de capacités de détection des menaces, d'investigation et d'intervention plus rapides. Elles peuvent utiliser les frameworks et les workflows spécifiquement conçus pour accélérer la détection, l'investigation et la réponse aux incidents. Les équipes de sécurité peuvent également utiliser des tableaux de bord prédéfinis, des rapports, des capacités d'investigation, des catégories de cas d'utilisation, des analyses, des recherches de corrélation et des indicateurs de sécurité pour simplifier la gestion des menaces et la gestion des incidents. Elles peuvent ensuite utiliser ces capacités pour établir une corrélation entre les logiciels en tant que service (SaaS) et les sources sur site pour découvrir et déterminer l'étendue de l'activité des utilisateurs, de l'activité réseau, de l'activité des points de terminaison, de l'activité d'accès et de l'activité anormale.

Splunk User Behavior Analytics (UBA) est une solution fondée sur le machine learning qui détecte les menaces inconnues et les comportements anormaux des utilisateurs, des points de terminaison et des applications. Elle renforce votre équipe de sécurité existante et la rend plus productive en détectant des menaces qui passeraient inaperçues en raison du manque de personnes, de ressources et de temps.

Les équipes de sécurité peuvent utiliser **Splunk UBA** pour améliorer la visibilité et la détection des menaces. Plus précisément, elles peuvent détecter les menaces internes et inconnues à l'aide d'algorithmes de ML non supervisés que les produits traditionnels de sécurité n'auraient pas détectées. Elles peuvent automatiser la corrélation des comportements anormaux en menaces haute fidélité à l'aide de visualisations sophistiquées de la kill-chain. Cette capacité permet aux équipes de passer plus de temps à rechercher les menaces grâce aux alertes basées sur le comportement de haute fidélité. Elles peuvent également identifier les dernières menaces sans interruption opérationnelle grâce aux mises à jour du contenu dynamiques par abonnement qui permettent aux équipes de sécurité de suivre l'évolution des dernières techniques de détection des menaces de manière proactive.

Splunk Phantom est une plateforme SOAR qui intègre les processus et les outils d'une équipe, leur permettant de travailler plus intelligemment, de répondre plus rapidement aux incidents et d'améliorer leurs défenses.

Phantom aide à maximiser les efforts des opérations de sécurité d'un SOC. Les équipes de sécurité peuvent automatiser les tâches répétitives pour optimiser leurs efforts et focaliser leur attention sur les décisions qui nécessitent vraiment un apport humain. Elles peuvent réduire les temps d'attente grâce à une détection et une investigation automatisées, et réduire les temps de réponse grâce à des procédures qui s'exécutent à la vitesse de la machine. Phantom aide également les équipes de sécurité à intégrer leur infrastructure de sécurité existante de manière à ce que chaque élément participe activement à la stratégie de défense du SOC.

À propos de Splunk.

Splunk Inc. rend vos données accessibles, utilisables et utiles pour tous.

Découvrez comment la suite Splunk pour les Opérations de sécurité peut vous aider à moderniser votre SOC dès aujourd'hui.

2020-Splunk-SEC-Fundamental-Guide-to-Building-a-Better-Security-Operations-Center-111-EM

splunk>
turn data into doing™