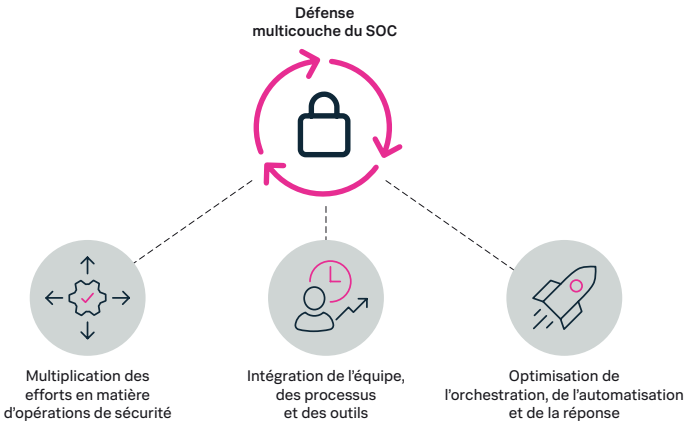
Splunk® Phantom

Optimisez l'efficacité de votre SOC grâce aux fonctionnalités d'orchestration, d'automatisation et de réponse de sécurité (SOAR)

- **Comblez vos lacunes de compétences en matière de sécurité** en multipliant vos efforts d'opérations de sécurité
- **Intégrez votre équipe, vos processus et vos outils** pour une efficacité accrue du SOC
- **Boostez votre SOC** grâce aux fonctionnalités avancées d'orchestration, d'automatisation et de réponse



Les équipes de sécurité travaillent dur pour identifier, analyser et lutter contre les menaces auxquelles leurs organisations sont confrontées.

Ces équipes sont également aux prises avec une ligne d'assemblage sans fin de produits spécifiques et de contrôles de sécurité statiques indépendants, sans aucune orchestration entre eux. Si l'on ajoute le fait que la plupart des entreprises n'ont pas assez de personnel pour analyser le volume de leurs alertes de sécurité quotidiennes, il en résulte un arriéré croissant d'incidents de sécurité.

Les organisations veulent mieux exploiter les ressources actuelles en déployant des outils qui offrent une efficacité maximale à grande échelle, tout en créant un système de défense unifié plus performant que la somme de ses parties.

Splunk Phantom offre des fonctionnalités d'orchestration, d'automatisation et de réponse de sécurité (SOAR) qui permettent aux analystes d'améliorer l'efficacité et de réduire les délais de réponse aux incidents. Les organisations sont en mesure d'améliorer la sécurité et de mieux gérer les risques en intégrant ensemble les équipes, les processus et les outils. Grâce à Phantom, les équipes de sécurité peuvent automatiser les tâches, orchestrer les workflows et prendre en charge un large éventail de fonctions de SOC, notamment la gestion des événements et des cas, la collaboration et la création de rapports.

Automatisation du SOC

Phantom permet aux équipes de travailler plus intelligemment en exécutant des actions automatisées à travers leur infrastructure de sécurité en quelques secondes, ce qui prendrait des heures si cela était effectué manuellement. Les équipes peuvent codifier les workflows dans les procédures automatisées de Phantom à l'aide de l'éditeur visuel (aucun codage requis) ou de l'environnement de développement Python intégré. En se déchargeant de ces tâches répétitives, les équipes peuvent se concentrer pleinement sur la prise de décisions essentielles.

Orchestration

Phantom est le tissu conjonctif qui permet aux outils de sécurité existants de mieux fonctionner ensemble. En connectant et en coordonnant des workflows complexes à travers l'équipe et les outils du SOC, Phantom garantit que chaque partie de la défense multicouche du SOC participe activement à une stratégie de défense unifiée. Une abstraction puissante permet aux équipes de se concentrer sur ce qu'elles doivent accomplir, tandis que la plateforme traduit cela en actions spécifiques à l'outil.

Réponse aux incidents

Phantom aide les équipes de sécurité à investiguer les menaces et à y répondre plus rapidement. En utilisant les fonctionnalités automatisées de détection, d'investigation et de réponse de Phantom, les équipes peuvent exécuter des actions de réponse à la vitesse de la machine, réduire le temps de séjour des malwares et réduire leur temps moyen de résolution (MTTR). Grâce à Phantom sur Splunk Mobile, les analystes peuvent désormais utiliser leur appareil mobile pour répondre aux incidents de sécurité pendant leurs déplacements. La fonctionnalité de gestion des événements et des cas de Phantom permet de rationaliser davantage les opérations de sécurité. L'activité et les données relatives aux cas sont aisément accessibles à partir d'un référentiel central. Les membres de l'équipe peuvent facilement discuter avec leurs collègues à propos d'un événement ou d'un cas, ainsi qu'attribuer des événements et des tâches à la personne appropriée.

Vous souhaitez en savoir plus ?
Téléchargez la **version Community gratuite** de Splunk Phantom et commencez dès aujourd'hui.

splunk>

En savoir plus : www.splunk.com/asksales

www.splunk.com

2020-sec-splunk-phantom-maximize-your-soc-efficiency-with-soar-pb-A4-108