Le guide essentiel des **procédures de sécurité fondamentales**

splunk>
turn data into doing™

Le Guide essentiel des procédures de sécurité fondamentales

Depuis des années, les responsables de la sécurité sont confrontés à d'innombrables défis : déluge d'alertes, rareté des talents, disparité des outils. Des équipes de sécurité aux ressources insuffisantes luttent pour prendre en charge un afflux incessant d'alertes de sécurité.
Il n'a jamais été aussi crucial de poser les fondements d'un centre des opérations de sécurité (SOC) solide et mature, bâti sur des procédures de sécurité normalisées exploitant l'automatisation et l'orchestration.

Essayez Splunk Phantom gratuitement

Ressources complémentaires

- Sam Hays, Community Manager technique senior pour Splunk Phantom
- Créez un compte pour rejoindre la communauté Slack de Splunk Phantom
- Splunk Answers
- Visite guidée de Splunk Phantom

Qu’est-ce qu’une procédure opérationnelle normalisée ?

Une procédure opérationnelle normalisée est un ensemble d’instructions écrites détaillées qui décrivent de quelle manière les employés ou les collaborateurs d’une équipe doivent accomplir des tâches de routine. Ces procédures doivent être concises, faciles à lire et à corriger si nécessaire.

Dans ce guide, les procédures opérationnelles standard de l’industrie de la sécurité seront appelées « procédures de sécurité normalisées » (PSN). Les PSN sont un outil stratégique pour toute équipe de sécurité compétente et mature. Elles jouent le rôle de règle d’or pour les analystes de sécurité expérimentés, mais aussi de workbook de formation pour les analystes juniors qui rejoignent l’équipe. Découvrons les principaux avantages des PSN pour les équipes de sécurité.

Les avantages des procédures de sécurité normalisées

Réduction du temps de réponse

Les PSN offrent à l’analyste de sécurité un ensemble établi et reproductible d’étapes qu’il peut accomplir de façon rapide et efficace en cas d’incident de sécurité. Lorsqu’un incident donné se produit, l’analyste peut commencer à réaliser les étapes de la PSN correspondante sans délai ou presque. Il ne perd pas de temps à déterminer quelle réponse apporter à différents types d’incidents.

Réduction de l’erreur humaine

Les analystes de sécurité opèrent souvent dans des conditions stressantes et urgentes. Malheureusement, cet environnement de « cocotte-minute » est un catalyseur d’erreurs chez l’analyste, erreurs qui peuvent faire la différence entre une résolution rapide et une faille coûteuse. Les analystes doivent réagir aux incidents de sécurité avec rapidité et précision pour réduire les risques de dommages pour l’entreprise. Muni d’une liste claire de procédures à suivre, l’analyste peut plus facilement faire preuve de concentration, de précision et de rapidité dans des conditions stressantes.

Mesurez la performance des équipes avec des SLA prévisibles

Les PSN aident les responsables de la sécurité à comprendre et établir des métriques de performance de référence pour certains événements spécifiques dont les temps de traitement sont prévisibles. Elles permettent ainsi à l’équipe de mettre en place des accords de niveau de service (SLA) et d’améliorer ses résultats en continu.

Contrôle qualité

Il est absolument crucial que le SOC maintienne une qualité constante dans la détection, l’investigation et la prise en charge de différents types d’événements de sécurité. Les PSN offrent un mécanisme pour suivre la hausse, la baisse ou la constance de la qualité de ces activités. Les directeurs de la sécurité informatique (RSSI) et les responsables de SOC peuvent avoir besoin de produire des rapports de performance pour la direction de l’entreprise.

Conformité

Des procédures bien écrites peuvent satisfaire certaines exigences de conformité réglementaires, et servir de liste de contrôle pour les audits.

Archives historiques

Grâce à des registres écrits ou électroniques des étapes accomplies au cours d’une enquête ou d’une procédure de résolution, en précisant à quel moment et de quelle manière, n’importe qui peut comprendre ce qui s’est passé, même si l’une des personnes impliquées quitte l’entreprise. Les connaissances « tribales », transmises oralement dans une organisation, disparaissent souvent sans une documentation correcte.

Directives de formation pour les nouveaux collaborateurs

Il est essentiel de proposer une documentation précise et concise aux nouveaux analystes de sécurité qui rejoignent l’équipe. Fournir des PSN aux nouveaux collaborateurs accélérera leur intégration.

Bâtir les fondations des opérations de sécurité

La mise en place de fondations solides pour votre équipe de sécurité n'est pas une tâche facile. De nombreux SOC ne comptent qu'un à cinq membres, chargés de traiter des centaines, voire des milliers d'alertes chaque jour. Pour optimiser son efficacité, l'équipe doit être totalement alignée sur des protocoles communs et mettre en œuvre un framework robuste pour les appliquer.

Coordination de l'équipe

L'un des grands défis que peut avoir à relever un responsable de SOC, notamment s'il examine avec honnêteté l'équipe qui gère les incidents de sécurité, est la différence de qualité de travail entre un analyste expérimenté et un analyste junior. Sans des procédures correctement documentées, les collaborateurs du SOC peuvent accomplir différentes étapes avec des degrés de rigueur variables lors de l'exploration et de la correction des alertes. De plus, certains membres de l'équipe n'expliquent pas toujours pourquoi certaines alertes font l'objet d'une enquête approfondie, tandis que d'autres sont closes sans explication. Cela peut avoir un impact négatif sur la position de sécurité globale de l'entreprise, car certaines alertes ne font pas l'objet d'une exploration suffisante ou adaptée.

Les responsables de la sécurité rêvent d'une équipe compétente, munie de procédures éprouvées et reproductibles pour traiter les incidents de tout type. Ces procédures permettent aux analystes chevronnés d'innover et de travailler par itération, tout en donnant aux analystes juniors les moyens d'enrichir leurs compétences. Les équipes performantes pratiquent l'amélioration par itération, l'innovation créative et les processus bien pensés pour combler les lacunes des nouveaux collaborateur et des juniors. En imposant la même norme à tous les membres de l'équipe, les responsables de la sécurité garantissent la qualité des résultats de leur équipe et produisent des indicateurs de performance clairs pour la direction en cas de besoin.

Pour assurer la régularité dans les résultats de l'équipe, Splunk Phantom, qui est une solution robuste d'orchestration, d'automatisation et de réponse de sécurité (SOAR), propose une fonctionnalité de workbook (manuel). Cette fonctionnalité décrit de quelle manière un humain doit agir (processus, marche à suivre, résultat, etc.) lorsqu'il est confronté à un problème, et elle peut être complétée, voire supplantée, par une automatisation. Techniquement, ces workbooks sont des procédures opérationnelles normalisées codifiées dans l'interface de Splunk Phantom, et ils délivrent des workflows normalisés.

Dans la section suivante, nous allons vous expliquer comment élaborer des PSN et les traduire en workbooks dans Splunk Phantom.

Rédaction des procédures de sécurité normalisées

1. Identification des processus

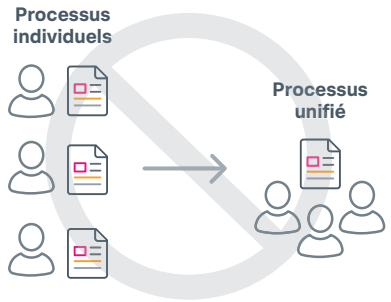
Commencez par identifier les processus de sécurité qui doivent être opérationnalisés et améliorés. L'équipe doit déterminer en concertation les processus qu'elle souhaite traiter en priorité. Le choix de la première PSN à normaliser est crucial. Si le résultat est bon (autrement dit, si la PSN permet à l'équipe de travailler plus vite et plus efficacement), cela accélérera l'adhésion de l'équipe aux concepts et aux avantages des PSN et la motivera à participer à l'implémentation des PSN dans un outil d'automatisation et d'orchestration.

Voici quelques principes de base pour choisir le processus de sécurité à normaliser :

1. Limitez-vous aux processus qui sont réalisés actuellement (à des approches établies, donc) pour permettre à l'équipe de produire du feedback de qualité.
2. Cherchez les processus accomplis fréquemment et connus de tous les membres de l'équipe.
3. Limitez les options aux processus qui présentent une pénalité importante en cas d'irrégularité.
4. Identifiez les processus qui pourraient, à l'avenir, bénéficier d'une automatisation afin de réduire le nombre de tâches manuelles exigées de l'analyste.
5. Pensez également aux processus associés à des obligations réglementaires ou de conformité, et pour lesquels la régularité apporte un bonus en termes d'audit.

2. Normalisation des processus

Une fois que vous avez trouvé un bon candidat, vous pouvez, en concertation avec votre équipe, l'analyser objectivement et normaliser le travail de chaque membre de l'équipe pour constituer un workbook codifié et applicable par tous les collaborateurs, afin de passer d'un ensemble de processus individuels à un seul processus unifié.



Mais avant toute normalisation, vous devez en premier lieu comprendre comment l'équipe fonctionne au quotidien. Voici les premières étapes à suivre pour parvenir à un processus unifié :

- **Recueillez des informations** sur la façon dont l'équipe travaille aujourd'hui en lui posant des questions sur le processus que vous avez choisi. Observez comment chaque membre de l'équipe gère ce type d'incident de façon indépendante.
- **Synthétisez tous les processus individuels** dans les notes.
- **Organisez une réunion d'équipe** pour étudier les différentes tâches accomplies par chaque membre pour remédier à l'incident. Comprenez les raisons pour lesquelles chaque membre a agi ou non de telle ou telle manière, l'a fait dans cet ordre particulier et selon quelle priorité.
- **Encouragez une discussion ouverte et saine**, échangez pour comprendre la perception de chacun concernant l'approche de cet incident de sécurité.
- **Convenez d'un ensemble de tâches optimal pour composer le processus** qui sera appliqué par tous les membres de l'équipe à l'avenir. Cette liste de tâches servira de squelette pour élaborer la documentation du workbook et sa codification dans Phantom.

3. Documentation du workbook

Muni de la liste des actions qui seront accomplies par tous les analystes à partir de maintenant (et recueillies au cours de la précédente réunion), vous pouvez maintenant élaborer le workbook (sur papier).

Pour élaborer le workbook sur papier :

- **Dressez la liste des actions identifiées en commun** lors de la précédente réunion d'équipe et distribuez-la aux collaborateurs.
- **Ceux-ci vont l'examiner de façon indépendante** et noter leurs éventuelles réflexions.
- **Ils vont ensuite la passer en revue collectivement** pour s'accorder sur une version.
- **Chaque analyste va utiliser cette version papier du workbook comme guide lors de la gestion des incidents réels.** Au cours de cette période, les analystes doivent disposer d'un temps suffisant pour tester la procédure et vérifier qu'aucun élément crucial n'a été omis, que rien de superflu n'a été ajouté et que tout peut être réalisé dans un délai raisonnable.
- **Organisez une nouvelle réunion d'équipe** après que tout le monde a eu le temps d'examiner la liste de tâches et de prendre des notes. Dans le cadre de cette réunion, cette liste de tâches doit devenir une liste ordonnée intégrant des stratégies de gain de temps appropriées.
- **Finalisez la liste de tâches** : lorsque vous codifierez ce workbook dans Splunk Phantom, vous devrez saisir les tâches et les grouper en « phases ». Votre workbook papier est terminé !

Une fois le workbook papier créé, il est bon que l'équipe prenne le temps d'examiner certains événements réels précédents pour confirmer que les vrais positifs auraient bien été détectés par le nouveau processus. N'oubliez pas qu'une cadence d'amélioration permanente doit être établie.

Enfin, une fois que toutes les parties prenantes sont satisfaites de la nouvelle procédure documentée, il est temps de passer à l'étape suivante et de la codifier dans Phantom. Référez-vous à la liste de contrôle fournie à la fin de ce guide pour vérifier que vous avez réalisé toutes les étapes requises pour créer une PSN.

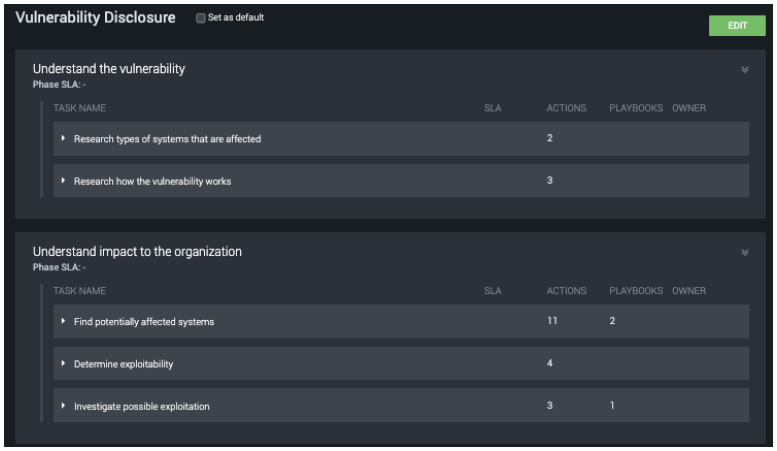
Création des workbooks dans Phantom

Vous avez posé les bases pour que votre équipe implémente le workbook papier dans Phantom, dans une optique d'automatisation future. Une fois cela fait, vous avez l'assurance que tous vos analystes vont appliquer les mêmes étapes à chaque fois qu'un incident se produit, ce qui se traduit par une régularité dans la réponse et une meilleure intégration de l'équipe.

Composants du workbook

Un workbook Phantom se décompose en plusieurs phases. Chacune de ces phases peut être associée à plusieurs tâches, accords de niveau de service, actions et procédures.

Idéalement, lorsque votre équipe et vous élaborez des workbooks, gardez à l'esprit que les phases représentent des étapes conceptuelles à réaliser, tandis que les tâches correspondent à des actions concrètes. Par exemple, si vous créez un workbook en cas de « vulnerability disclosure » (divulgation de vulnérabilité), vous pouvez le structurer comme suit :



Création d'un workbook Phantom

1. Phantom est fourni avec des workbooks prédéfinis, disponibles sous **Administration** > **Paramètres du produit** > **Workbooks**. Vous trouverez également un bouton pour créer de nouveaux workbooks dans cette vue.

2. Cliquez sur le bouton + WORKBOOK pour être redirigé vers l'écran de création de workbook.

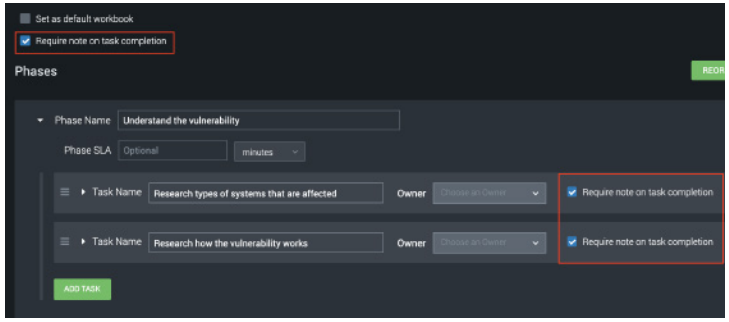
3. Saisissez le « Workbook Name» (Nom du workbook) et la « Workbook Description » (Description du workbook).

4. Lorsque vous créez ou modifiez un workbook, deux options de configuration vous demandent de prendre une décision.

« Set as default workbook» (Définir comme workbook par défaut) : si vous convertissez un événement en dossier sans lui affecter un autre workbook, ou si vous créez un dossier manuellement sans spécifier de workbook, celui-ci sera appliqué par défaut.

« Require note on task completion »(Exiger des notes en fin de tâche) : cette option sera activée pour chaque tâche de chaque phase.

5. Vous pouvez ensuite commencer à saisir le contenu de votre workbook papier sous forme de phases et de tâches dans Splunk Phantom. Vous avez également la possibilité d'attribuer différents responsables à chaque tâche. Si les analystes sont organisés selon une structure hiérarchique (par exemple, niveau 1/niveau 2, ou junior/senior) qui doit déterminer qui accomplit chaque tâche, vous devez l'indiquer dans la configuration. Comme nous allons le voir dans la section suivante, Splunk Phantom permet d'affecter des tâches en fonction **de l'utilisateur ou du rôle**, et ce concept est important si l'équipe n'est pas entièrement horizontale.



Si l'option «Require note on task completion» est activée, un analyste qui travaille sur une tâche ne peut pas la clore sans saisir des remarques. Le réglage du même nom sur l'écran du workbook (voir capture d'écran ci-dessus) permet simplement d'activer cette option pour chaque tâche de chaque phase. C'est particulièrement utile si l'équipe souhaite avoir la possibilité de réaliser une analyse rétroactive approfondie de chaque événement ou dossier.

6. Passez en revue chaque section et terminez de saisir votre workbook papier dans Splunk Phantom. Une fois que vous avez terminé, enregistrez-le dans le système.

7. Une fois que le workbook est configuré comme vous le souhaitez, il peut être intéressant de l'appliquer à quelques incidents de test, et de demander à l'équipe de faire de même. Cela vous donnera l'occasion de vous familiariser avec l'interface utilisateur des workbooks de Splunk Phantom.

Application des workbooks Phantom aux incidents

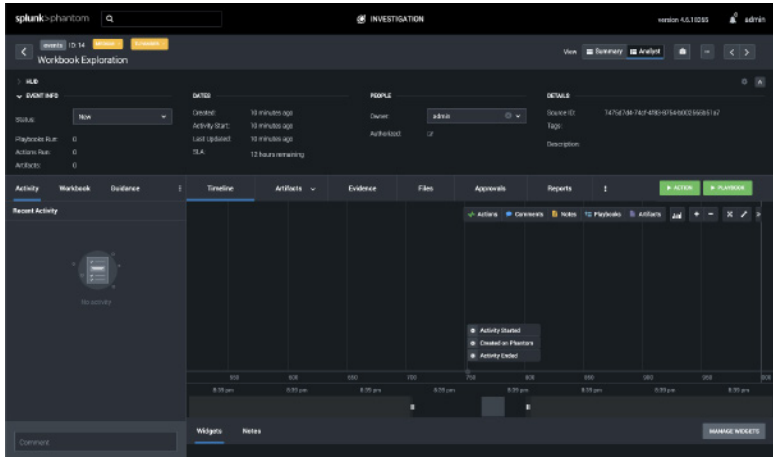
Une fois le workbook créé, vous pouvez commencer à l'intégrer dans votre workflow de réponse à un événement.

Créez un événement

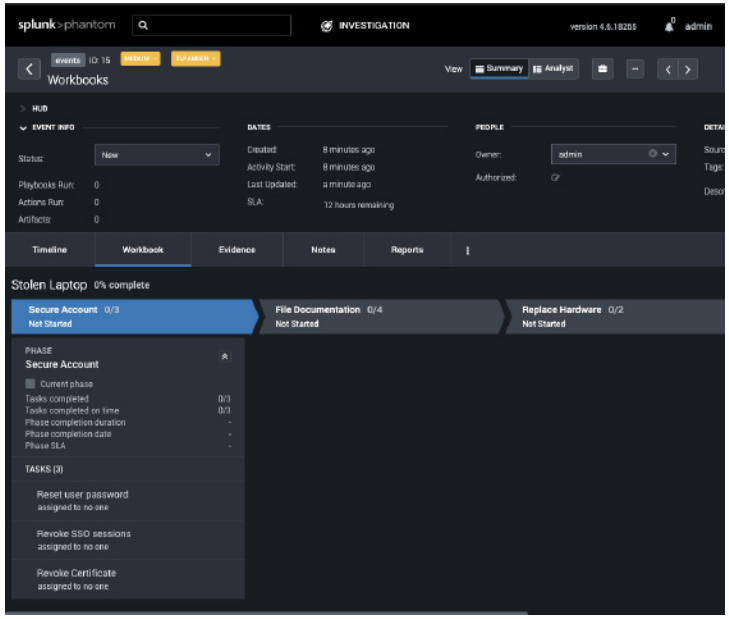
1. Rendez-vous dans **Administration** > **Sources.**
2. Cliquez sur + EVENT sur la page des sources.
3. Remplissez la fenêtre « Add event » (Ajouter un événement) en indiquant :
   a. Nom de l'événement : un nom court et simple (par exemple, « Mary Smith »).
   b. Étiquette : « phishing evaluation » (évaluation d'hameçonnage) (cette étiquette aura son importance ultérieurement).
   c. Type d'événement : dossier (cela vous permettra d'appliquer votre workbook à l'événement).
   d. ...les autres paramètres conservent leurs valeurs par défaut.
4. Cliquez sur « Save» (Enregistrer) pour créer le nouvel événement.

Ajoutez le workbook à l'événement

1. Ouvrez le nouvel événement que vous venez de créer.
2. Vous voyez « Activity », « Workbook » et « Guidance » dans l'angle inférieur gauche de l'écran. Lorsque vous cliquez sur « Workbook », vous pouvez « Add workbook » pour activer le workbook que vous venez de créer. Une fois que c'est fait, l'onglet Workbook inclut les phases et les tâches que vous avez définies. Vérifiez que vous êtes bien en « Analyst view » (vue analyste). .



3. Vous (en tant qu'analyste) pouvez désormais parcourir les tâches de chaque phase, prendre des notes et ajouter des fichiers si nécessaire. C'est le cadre qui doit vous permettre d'assurer une cohérence et une régularité dans la façon dont chaque membre de l'équipe gère chaque type d'incident.



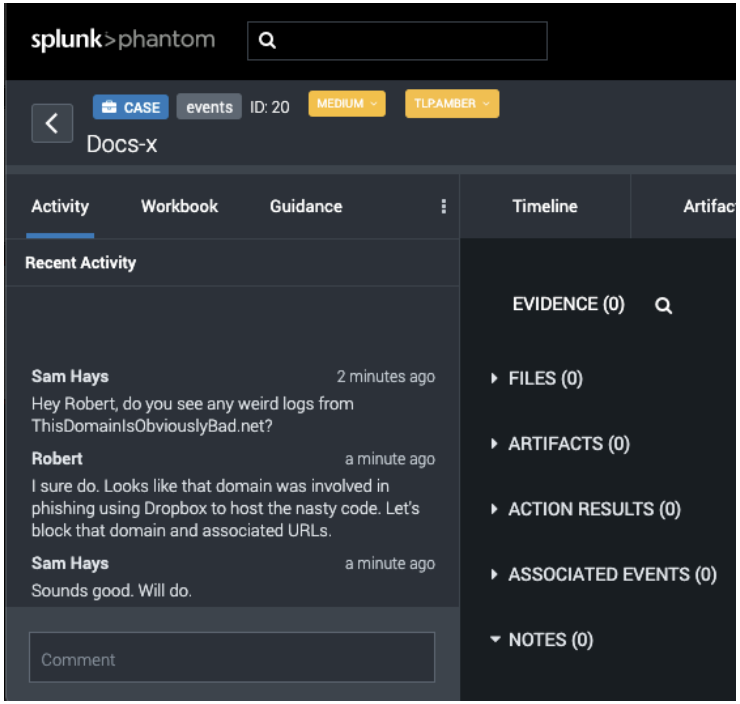
Collaboration avec l'équipe sur un événement

Lors du traitement d'un événement, Splunk Phantom permet une interaction directe entre les collaborateurs au sein de cet événement. Cela prend principalement trois formes : «Activity, Notes et Evidence» (activité, notes et preuves).

1. Activité

Vous pouvez voir le volet « Activity » sur le côté gauche de l'écran lorsque vous affichez un événement. Les analystes peuvent discuter des étapes de remédiation en temps réel au sein de l'environnement Phantom. Cela leur évite de recourir à un environnement de discussion externe au cours d'une investigation, tout en maintenant le contexte de l'incident dans Phantom. Cette fonctionnalité peut être utile pour tenir d'autres membres de l'équipe informés d'un incident particulier, car elle leur permet de revoir la discussion.

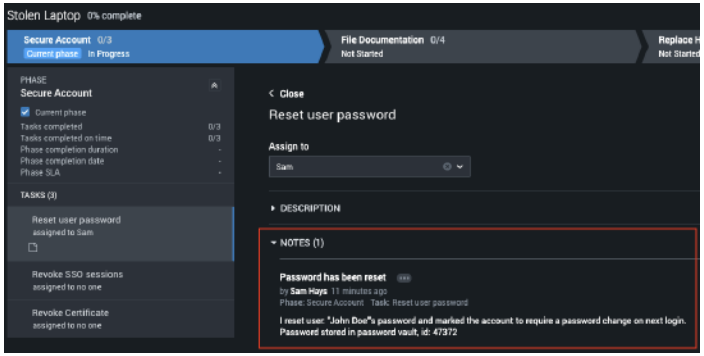
Disposer d'une plateforme de discussion interne pour aborder les informations sensibles associées à un incident aide également l'équipe à respecter ses obligations de conformité réglementaire. Si une équipe travaille sur une enquête de sécurité et doit discuter d'un utilisateur ou de ses attributs, elle peut être amenée à manipuler des informations personnellement identifiables (IPI). Les données de ce type sont protégées par plusieurs lois et doivent être traitées avec les plus grandes précautions. Pour cette raison, conserver les données dans Phantom évite de devoir comprendre les Politiques de confidentialité des autres systèmes de conversation.



2. Notes

Si la communication en temps réel est parfaitement adaptée au volet des activités, des informations structurées doivent être consignées sous la forme de notes pour faciliter la lecture et la consultation ultérieure. Phantom propose plusieurs catégories de notes à cette fin.

- **Task notes (notes de tâches) :** lorsqu'un analyste suit un workbook, il peut souhaiter fournir des descriptions détaillées, à titre personnel ou à l'intention de l'équipe. Ces notes délivrent un récit intelligible de sorte qu'un autre analyste en charge de répondre à l'incident n'aura pas besoin d'explorer les logs ni les données machine pour en comprendre le détail.
- **General notes (notes générales) :** vous pouvez ajouter des notes générales au dossier. Ces notes peuvent servir à préciser le contexte de l'événement et facilitent la compréhension du scénario dans sa globalité. C'est aussi là que l'on peut ajouter des informations disparates.

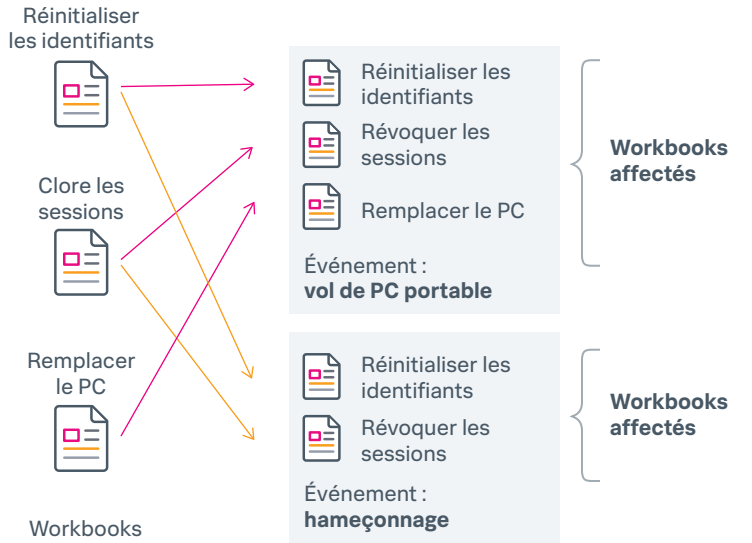


3. Evidences (Preuves)

Lorsqu'un analyste suit différentes pistes lors d'une investigation, beaucoup d'entre elles s'avèrent être des impasses mais certaines produisent des résultats pertinents. Toutes les pistes suivies seront vraisemblablement documentées, mais cela crée du bruit qu'il faut filtrer pour trouver les informations intéressantes. Pour éliminer ce problème, il est possible de « marquer comme preuve » certaines notes. La note apparaît alors dans le volet des preuves. Une fois qu'elle s'y trouve, les conclusions les plus « intéressantes » d'une investigation sont faciles à passer en revue. Le volet des preuves peut inclure plusieurs éléments, comme des fichiers provenant du dépôt, des artefacts, des résultats d'actions, des événements associés et des notes.

Workbooks appliqués à plusieurs dossiers

Contrairement à bien d'autres produits SOAR concurrents, Phantom permet à l'analyste d'appliquer plusieurs workbooks à un incident ou un événement. Cela permet d'adopter une approche modulaire et structurée dans la conception des workbooks.



De cette manière, si vous créez des workbooks qui correspondent à un ensemble d'actions défini, vous pouvez les réutiliser dans un grand nombre de scénarios d'utilisation. Mieux encore, lorsque ces actions changent (par exemple parce que le système LDAP a changé de type), la mise à jour d'une procédure sera propagée à tous les prochains incidents utilisant le workbook.

Étude de cas : Hameçonnage ou non ?

L'équipe Splunk Phantom travaille avec des clients du monde entier pour les aider à optimiser leurs opérations de sécurité. L'exemple suivant est un cas d'utilisation réel qui décrit la tâche entreprise par une société dans le cadre de son adoption d'une approche SOAR avec Splunk Phantom.

Contexte : cette équipe de sécurité comprend un responsable et cinq analystes possédant différents niveaux de compétence et chargés de répondre aux incidents. Pendant la phase initiale de sélection du processus, l'équipe a décidé que parmi toutes les tâches et missions de sécurité, l'hameçonnage représentait le meilleur choix selon les critères de sélection indiqués plus haut dans ce guide. C'est donc sur ce processus qu'ils ont décidé de travailler en premier.

Le scénario : l'entreprise a configuré une boîte de réception appelée « la mare », où tous les employés ont reçu l'instruction d'envoyer les e-mails suspects (sous la forme d'une pièce jointe). Les utilisateurs savaient également qu'ils ne doivent rien faire d'autre avant d'avoir reçu une réponse de l'équipe de sécurité qui leur dira s'ils peuvent ou non interagir avec le message d'origine.

À ce stade, l'équipe a réalisé les étapes suivantes :

1. Sélection du processus à opérationnaliser avec Splunk Phantom (hameçonnage).
2. Collecte d'informations sur la façon dont le processus est exécuté par chaque membre de l'équipe.
3. Synthèse des résultats de l'étape deux avec l'équipe pour élaborer un workflow standard.
4. Application du nouveau workflow à des exemples de cas.
5. Implémentation du workbook dans Splunk Phantom.

Exemple de workbook en cas d'hameçonnage

Phase de collecte des données :

1. La personne d'astreinte (« responder ») supervise activement la boîte de réception pendant les heures de travail. Lorsqu'un nouvel e-mail arrive dans la boîte, l'intervenant crée un nouvel événement dans Phantom, sous l'étiquette « Phishing Evaluation « (évaluation d'hameçonnage).

2. L'intervenant télécharge une copie de l'intégralité du message depuis la boîte de réception et la joint au dépôt de l'événement créé (à des fins d'archivage et pour les prochaines phases).

    a. L'intervenant ouvre l'e-mail dans un éditeur de texte (ou une application sécurisée) pour l'examiner.

Phase d'investigation :

3. L'intervenant évalue le contexte du corps du message.

    a. Si les formulations trahissent un danger manifeste, il doit ensuite :

        i. Convertir l'événement en dossier en lui attribuant une priorité élevée
        ii. Créer une note détaillant les conclusions
        iii. Ajouter une note au tableau des preuves
        iv. Terminer la phase d'investigation

    b. Autrement :

        i. Il passe à l'étape 4.

4. L'intervenant capture tous les hyperliens du corps du message.

5. Chaque hyperlien recueilli est évalué dans VirusTotal.

    a. Si le score est positif, l'intervenant va :

        i. Convertir l'événement en dossier en lui attribuant une priorité élevée
        ii. Ajouter une note contenant des détails
        iii. Marquer la note comme preuve
        iv. Terminer la phase d'investigation

    b. Autrement :

        i. Il passe à l'étape 6.

6. Chaque hyperlien recueilli est ouvert dans un service cloud de sandbox et évalué.

    a. S'il s'avère malveillant, l'intervenant va :

        i. Convertir l'événement en dossier en lui attribuant une priorité élevée
        ii. Ajouter une note contenant des détails
        iii. Marquer la note comme preuve
        iv. Terminer la phase d'investigation

    b. Autrement :

        i. Il passe à l'étape 7.

7. L'intervenant d'astreinte vérifie l'âge du domaine.

    a. S'il a moins d'un an, il va :

        i. Convertir l'événement en dossier en lui attribuant une priorité Intermédiaire
        ii. Ajouter une note contenant des détails
        iii. Marquer la note comme preuve

    b. Autrement :

        i. Il passe à l'étape 8.

Phase de décision et de réponse :

8. L'intervenant va :

    a. Consigner ses conclusions dans une note

    b. Marquer la note comme preuve

    c. Répondre à l'utilisateur par e-mail en lui communiquant ses conclusions

        i. Si elles sont mauvaises, l'utilisateur reçoit l'instruction de détruire l'e-mail.
        ii. Si le domaine est récent (mais qu'aucun autre indicateur suspect n'est présent), l'analyste doit donner son instruction en s'appuyant sur son jugement.
        iii. Si aucun signe de malveillance n'est détecté, l'utilisateur est autorisé à ouvrir l'e-mail tout en faisant preuve de prudence.

    d. Clôture de l'incident

Maintenant que chaque tâche de notre workbook papier est représentée dans Phantom, nous disposons d'un workbook qui améliore considérablement la cohérence de la réponse de l'équipe. Un processus établi est désormais en place. Cela a plusieurs avantages :

1. Nous savons quoi attendre de l'équipe.

2. Nous pouvons évaluer le temps nécessaire à différents membres de l'équipe pour accomplir des tâches similaires.

3. Nous pouvons commencer à suivre des métriques pour ce type d'incident.

4. Aucune étape n'est omise ni ignorée.

5. La répartition des responsabilités est clairement établie.

6. Nous avons mis en place les fondements d'une automatisation qui pourra réduire considérablement le temps nécessaire à l'exploration d'un soupçon d'hameçonnage.

Dans ce guide, nous avons vu l'importance d'assurer la cohérence de l'équipe des opérations de sécurité en évaluant et en harmonisant des PSN reproductibles. Cela permet en effet à votre équipe de produire des résultats de qualité à chaque fois. Bien que la création de procédures fondamentales des opérations de sécurité ne soit pas une tâche facile, elle est essentielle à la réussite du SOC car elle accroît la qualité, la vitesse et la précision de la réponse. Les entreprises qui cherchent non seulement à renforcer leurs opérations de sécurité grâce à des procédures normalisées, mais également à gagner en efficacité grâce à l'automatisation et l'orchestration, ont tout intérêt à commencer à poser des bases en structurant les opérations de sécurité fondamentales dans Splunk Phantom. Voici quelques points clés à garder en tête lorsque vous commencerez à mettre en œuvre des procédures de sécurité normalisées robustes avec votre équipe de sécurité.

À retenir

Toutes les équipes d'opérations de sécurité ne se ressemblent pas. Les équipes peu matures utilisent des processus ad-hoc, une automatisation limitée et peu d'outils. Les équipes ayant atteint un stade de maturité intermédiaire emploient en partie des processus et des politiques codifiés, mais il leur manque des moyens cohérents de mesurer et superviser les performances. Les équipes de grande maturité appliquent des procédures formelles et exploitent l'orchestration et l'automatisation pour un maximum d'efficacité et de précision. Atteindre ce degré de maturité exige un travail préalable qui inclut la création de PSN. Les équipes de sécurité qui cherchent à optimiser leur workflow et leurs performances ont tout intérêt à suivre ce guide pour gagner en maturité.

Il est indispensable d'obtenir l'adhésion et la participation de l'équipe dès le départ, car tout porte à croire que le personnel aura des idées pour réduire le délai de réponse, améliorer le processus d'investigation et innover sur d'autres types d'incidents par la suite. Si l'équipe n'a pas le sentiment que l'outil va simplifier et accélérer son travail, la création des procédures de sécurité normalisées et leur implémentation sera un combat permanent.

Le travail minutieux d'élaboration des procédures de sécurité normalisées demande un engagement mais il va considérablement améliorer la position de sécurité globale de l'entreprise. Ces processus vont contribuer à réduire le temps moyen de réponse et l'erreur humaine, tout en permettant une supervision cohérente de la qualité et de la conformité.

Essayez Splunk Phantom gratuitement

Ressources complémentaires

- Sam Hays, Community Manager technique senior pour Splunk Phantom
- Créez un compte pour rejoindre la communauté Slack de Splunk Phantom
- Splunk Answers
- Visite guidée de Splunk Phantom

Liste de contrôle de l'élaboration des procédures de sécurité normalisées

Suivez les étapes ci-dessous pour accompagner votre équipe de sécurité dans la création de PSN fondamentales et parvenir un maximum d'efficacité et de précision.

- ☐ **Listez** les processus de sécurité susceptibles d'être normalisés
- ☐ **Identifiez** le processus de sécurité que vous voulez commencer à normaliser.
- ☐ **Examinez** de quelle manière chaque membre de l'équipe traite le processus de sécurité choisi. Parlez à chaque membre de l'équipe de la façon dont il traite personnellement ce type d'événement, puis collectivement.
- ☐ **Documentez les différentes tâches** accomplies par chaque membre de l'équipe.
- ☐ **Organisez une réunion de « révision des tâches »** et rassemblez toutes les tâches dans une liste maîtresse.
- ☐ **Produisez une liste de tâches définitive** et donnez-la à chaque collaborateur pour qu'il la valide. Examinez les scénarios en groupe pour vérifier que rien ne manque.
- ☐ **Validez la liste finale** en demandant à chaque membre de l'utiliser pour valider des événements et vérifier que rien n'a été omis et que rien de superflu n'a été ajouté.
- ☐ **Répétez l'opération jusqu'à ce que la liste soit achevée.**
- ☐ **Activez la liste finale de tâches** en l'implémentant dans un workbook Phantom.

Liste de contrôle de l'implémentation des workbooks dans Phantom

Utilisez la liste de contrôle ci-dessous pour vous assurer de ne manquer aucune étape lorsque vous êtes prêt à transférer votre liste finale de tâches dans un workbook Phantom. Vous pouvez vous référer à la section du guide ci-dessus intitulée « Création des workbooks dans Phantom » pour les détails de la mise en œuvre.

- ☐ **Finalisez une version écrite du workbook** pour l'appliquer à un événement de sécurité décidé par l'équipe en concertation.
- ☐ **Testez le workbook** sur de nouveaux événements réels afin de déterminer les faux-positifs, les faux-négatifs, les vrais-positifs et les vrais-négatifs, et ainsi savoir si le workbook est opérationnel.
- ☐ **Déterminez les SLA, les délais de réponse et les notes** à saisir pour chaque tâche dans le workbook.
- ☐ **Saisissez le workbook dans Phantom.**
- ☐ **Créez un événement.**
- ☐ **Ajoutez un workbook à l'événement.**
- ☐ **Exécutez le workbook.**
- ☐ **Identifiez les portions du workbook qui peuvent être automatisées.**
- ☐ **Créez des procédures automatisées pour des tâches ou des événements spécifiques** (examen d'une adresse IP dans VirusTotal par exemple).
- ☐ **Intégrez les procédures dans les workbooks** pour réduire le temps de correction.

En savoir **plus.**

Splunk Phantom est une technologie d'orchestration, d'automatisation et de réponse de sécurité (SOAR) qui peut aider votre équipe de sécurité à travailler plus intelligemment et à réagir plus rapidement, pour renforcer votre position de sécurité globale.

Splunk Phantom

splunk>

AW-20-13568-SPLK-EssentialGuidetoFoundationalSecurityProcedures-11x9-105-EG