Orchestration de la sécurité : les principaux cas d'usage

Sommaire

Orchestration de la sécurité : tour d'horizon **3**
Traitement des alertes de sécurité **4**
Prévention et protection anti-phishing 4
Infection des terminaux par malware 5
Échecs de connexion utilisateur 6
Authentification depuis un lieu inhabituel 7
Gestion des opérations de sécurité **8**
Gestion des certificats SSL 8
Diagnostic des terminaux et démarrage des agents 9
Gestion des vulnérabilités 10
Traque des menaces et réponse à incident **11**
Recherche rapide d'IoC 11
Analyse des malwares 12
Réponse à incident orientée cloud 13
Automatisation de sécurité adaptable **14**
Enrichissement contextuel des IoC 14
Attribution d'un niveau de gravité aux incidents 15

Orchestration de la sécurité : tour d'horizon

Orchestration de la sécurité : de quoi parle-t-on ?

L'orchestration de la sécurité consiste à interconnecter des outils, des équipes et des infrastructures de sécurité disparates de façon à fluidifier les processus des opérations de sécurité et des réponses à incident. L'orchestration de la sécurité est un puissant levier d'automatisation et d'évolutivité dans la mesure où elle favorise l'interconnexion des systèmes.

Elle repose sur trois piliers : l'humain, les processus et les technologies. L'orchestration de la sécurité rationalise les processus de sécurité et connecte une variété d'outils et de technologies de sécurité, tout en maintenant un juste équilibre entre automatisation et intervention humaine. Les professionnels de la sécurité sont ainsi mieux armés pour renforcer la sécurité globale de l'entreprise.

Quelle est sa raison d'être ?

L'orchestration de la sécurité a pour vocation de résoudre un certain nombre de problèmes issus de différentes tendances et dynamiques du marché :

- **Hausse du nombre d'alertes :** l'extension permanente de la surface d'attaque, le nombre croissant de points d'entrée et la multiplication d'outils de cybersécurité spécialisés se traduisent par une augmentation constante du volume d'alertes. Pour éviter le burn-out, les analystes ont besoin de moyens d'identifier les faux positifs, d'éviter la duplication des incidents et de réduire le nombre d'alertes.
- **Prolifération des produits :** les analystes emploient de nombreux outils de sécurité et autres pour coordonner et traiter les réponses aux incidents. Conséquence : des passages incessants d'un écran à l'autre, un éparpillement des informations et un manque de cohérence dans la documentation des évènements.
- **Pénurie de compétences :** en sous-effectif permanent, les centres opérationnels de sécurité (SOC) assument une charge de travail croissante, source de stress et d'erreurs pour les équipes en place. Et la situation devrait encore s'aggraver puisque d'après les prévisionnistes, des millions de postes d'analystes sécurité resteront non pourvus dans les prochaines années.
- **Hétérogénéité des procédures de réponse :** dans un SOC mature, les équipes de sécurité passent le gros de leur journée à gérer l'urgence. Ils manquent de temps pour standardiser les procédures de réponse ou identifier les séquences propices à l'automatisation. La qualité et l'efficacité des réponses restent donc très aléatoires dans la mesure où elles varient en fonction de chaque analyste.

Quels avantages en attendre ?

Accélération de la réponse à incident

En automatisant les tâches manuelles de routine, l'orchestration de la sécurité peut accélérer et accroître la précision des réponses à incident, tout en améliorant la satisfaction professionnelle des analystes.

Standardisation et évolutivité des processus

Grâce à des workflows reproductibles dont les étapes sont clairement définies, l'orchestration de la sécurité peut faciliter la standardisation de l'enrichissement contextuel des incidents et des processus de réponse. Ces derniers gagnent alors non seulement en qualité mais aussi en évolutivité.

Unification des infrastructures de sécurité

Une plateforme d'orchestration de la sécurité fait office de tissu connectif entre des produits de sécurité auparavant disparates. Les analystes disposent ainsi d'une console centralisée depuis laquelle ils peuvent piloter la réponse à incident.

Gains de productivité pour les analystes

Avec l'automatisation des tâches de routine et la standardisation des processus, les analystes s'affranchissent des activités rébarbatives pour se recentrer sur des missions plus stratégiques et sur l'amélioration de leur sécurité.

Rentabilisation des investissements existants

Grâce à l'automatisation des actions répétitives et à la réduction des allers-retours entre consoles, l'orchestration de la sécurité permet aux équipes de coordonner facilement une multitude de produits et d'extraire davantage de valeur des équipements de sécurité existants.

Renforcement global de la sécurité

La conjugaison de tous ces avantages se traduit par un renforcement global de la sécurité de l'entreprise et par la baisse correspondante de son exposition au risque.

Figure 1 : Avantages de l'orchestration de la sécurité

Expressions à connaître

Playbooks

Les playbooks sont des ordonnanceurs de tâches établissant une représentation graphique des processus transverses aux différents produits de sécurité. Ces playbooks peuvent être automatisés, semi-automatisés ou 100 % manuels.

Intégrations

Les intégrations (ou applications) sont des mécanismes permettant aux plateformes d'orchestration de la sécurité de communiquer avec d'autres produits. Ces intégrations sont réalisées par l'intermédiaire d'API REST, de webhooks et d'autres techniques. Une intégration peut être unidirectionnelle ou bidirectionnelle, cette dernière permettant à un produit d'exécuter des actions sur un autre, et réciproquement.

Penchons-nous désormais sur quelques cas d'usage où l'orchestration de la sécurité permet de simplifier, d'automatiser et d'améliorer les réponses à incident et les opérations de sécurité.

Traitement des alertes de sécurité

Prévention et protection anti-phishing

Insuffisances actuelles

Les e-mails de phishing figurent parmi les cyberattaques les plus courantes. À la fois simples à exécuter et d'une redoutable efficacité, ils visent aujourd'hui les entreprises de toutes tailles. Sachant que plus de 90 % de toutes les compromissions de données commencent par un e-mail de phishing, le risque financier est bien réel.

Pour répondre à ces attaques, les analystes de sécurité doivent surmonter de nombreuses difficultés : traiter de multiples attaques sans se faire déborder, jongler constamment entre différents écrans de contrôle, éviter les erreurs dans l'exécution des tâches de routine, standardiser les procédures de réponse et de reporting, etc.

Intérêt de l'orchestration

Les plateformes d'orchestration de la sécurité peuvent recourir à des « playbooks de phishing » qui exécutent les tâches répétitives à vitesse machine, identifient les faux positifs et préparent le SOC à une réponse standardisée et cohérente à grande échelle. En particulier, l'identification et la résolution rapides des faux positifs permet aux analystes de se recentrer sur les véritables attaques pour qu'aucune ne passe entre les mailles du filet.

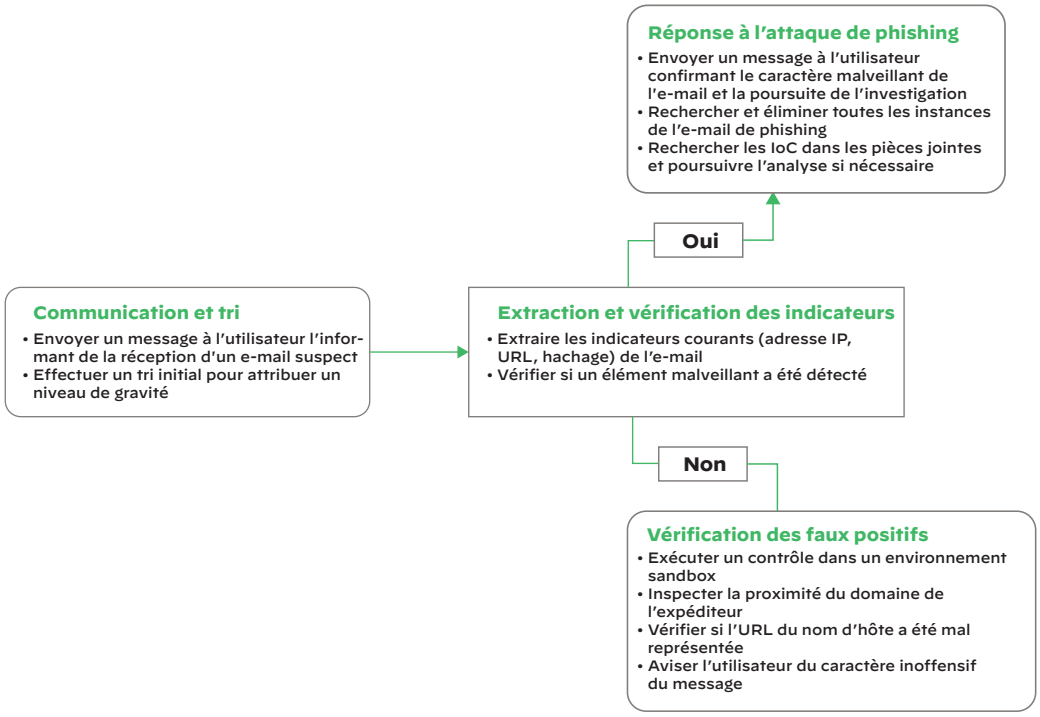

Figure 2 : Playbook de phishing

Ingestion

Une plateforme d'orchestration peut ingérer les e-mails suspects à partir d'une diversité de sources de détection, par exemple les systèmes de gestion d'informations et d'évènements de sécurité (SIEM) ou les services de journalisation. Lorsque le SOC regroupe tous les e-mails suspectés de phishing dans une boîte mail commune, ses équipes peuvent alors configurer l'intégration d'un « écouteur d'e-mails » sur la plateforme d'orchestration pour ingestion.

Une fois l'e-mail ingéré, un playbook est déclenché pour automatiser les étapes d'enrichissement des données et de réponse.

Enrichissement contextuel des données

Pour informer l'utilisateur concerné, le playbook lui envoie automatiquement un e-mail lui indiquant que l'e-mail suspect est en cours d'investigation. Le playbook peut alors prévoir deux actions pour l'enrichissement contextuel des données : 1. le **tri** et 2. l'**extraction des indicateurs de compromission (IoC)**.

En analysant les « ingrédients » de l'e-mail, à savoir son objet, son adresse d'origine, ses pièces jointes et autres, le playbook lui attribue un niveau de gravité par recoupement avec des référentiels de menaces externes. Ensuite, le playbook extrait les IoC de l'e-mail et recherche d'éventuels signalements dans les outils de Threat Intelligence du SOC.

Une fois cet enrichissement réalisé, le playbook vérifie si des indicateurs de malveillance ont été détectés. En fonction du résultat, différents axes de réponse peuvent être envisagés.

Réponse

Le playbook prévoit différents axes de réponse en fonction des éléments malveillants détectés dans l'e-mail suspect.

En cas de présence de tels éléments, le playbook envoie à l'utilisateur touché un e-mail contenant des instructions supplémentaires. Le playbook analyse également l'ensemble des boîtes mail / terminaux de l'organisation pour identifier les autres instances de l'e-mail incriminé, les supprimer et neutraliser l'attaque. Pour finir, le playbook ajoute les IoC observés aux listes noires des autres outils du SOC.

À l'inverse, si aucun élément malveillant n'est détecté, le principe de précaution impose de faire preuve de prudence avant de confirmer l'innocuité de l'e-mail. Le playbook vérifie les éventuelles pièces jointes à l'e-mail et les détone dans une sandbox pour étudier leur comportement. Si cette analyse ne renvoie aucune alerte, le playbook peut passer la main à des analystes qui procèdent à des investigations manuelles et qualitatives. Une fois que ces analystes ont confirmé le caractère inoffensif de l'e-mail, le playbook envoie un e-mail à l'utilisateur concerné pour l'aviser qu'il s'agit d'une fausse alerte.

Infection des terminaux par malware

Insuffisances actuelles

La protection des terminaux est une composante essentielle de la réponse à incident. Le problème, c'est que son implémentation est un parcours semé d'embûches. Les équipes de sécurité doivent souvent composer avec une diversité d'outils de protection des terminaux et autres instruments de sécurité, ce qui les oblige à jongler entre une multitude de consoles et à consacrer un temps précieux à des tâches manuelles répétitives. Même pour la seule protection des terminaux, les SOC utilisent parfois plusieurs outils, ce qui complique d'autant les recoupements de données entre chacun.

Intérêt de l'orchestration

Les playbooks d'orchestration de la sécurité peuvent unifier en un même workflow les processus entre les systèmes SIEM et les outils pour terminaux. De la sorte, les étapes répétitives peuvent être automatisées et les analystes n'interviennent que plus tard dans le processus pour prendre des décisions clés et mener des investigations.

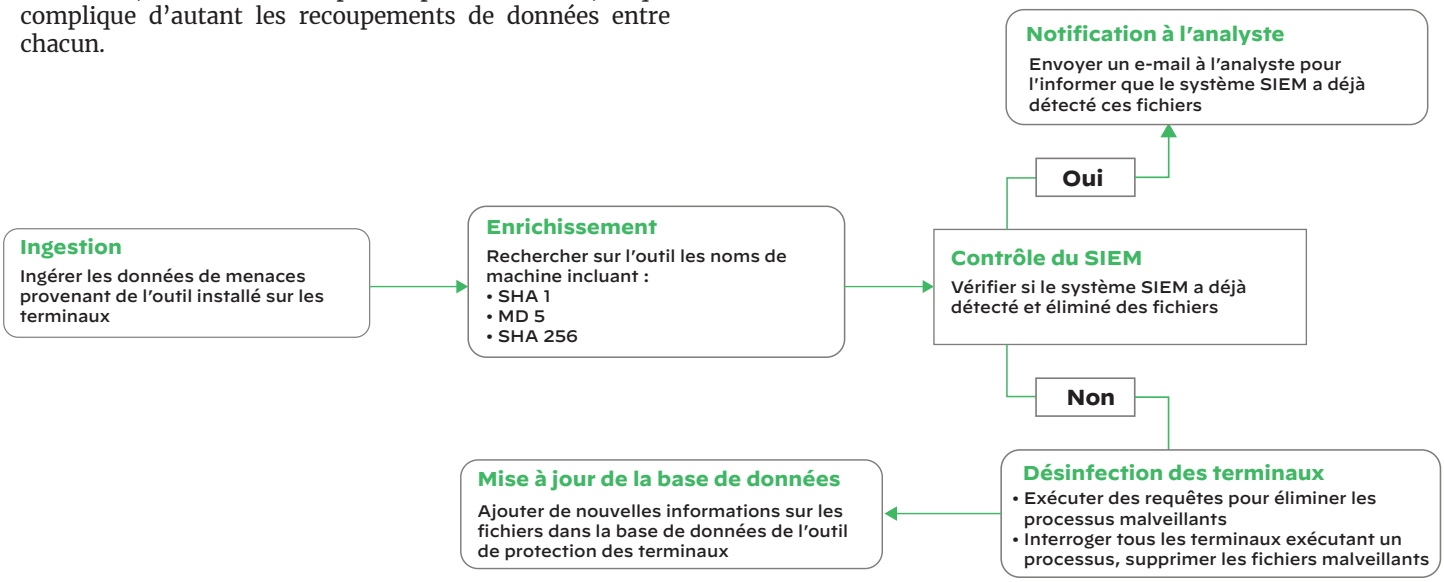

Figure 3 : Playbook de réponse à une infection de terminaux par malware

Ingestion

Le playbook ingère les flux de données de menaces provenant d'un outil de protection des terminaux (par exemple via l'API CrowdStrike Streaming).

Enrichissement contextuel des données

Le playbook interroge l'outil de protection des terminaux à la recherche de noms de machine / terminal présentant des indicateurs de malveillance (SHA1, MD5, SHA256 et autres).

Recoupement avec les données du SIEM

Le playbook recoupe les données des fichiers/hachages récupérés avec les données du SIEM, puis vérifie si des indicateurs ont été détectés et résolus par des actions du SIEM. Il signale ensuite à l'analyste si ces actions ont déjà permis de résoudre certains des éléments malveillants identifiés.

Désinfection des terminaux

Pour tous les indicateurs non détectés par le SIEM, le playbook communique avec le même outil de protection des terminaux, ou un autre (comme Tanium), pour exécuter des requêtes sur tous les terminaux. Entre autres fonctions, ces requêtes peuvent interrompre tous les processus malveillants ou éliminer les fichiers infectés, selon les fonctionnalités de l'outil de protection des terminaux.

Mise à jour de la base de données

Une fois les requêtes exécutées, le playbook ajoute les indicateurs en question à la base de données de l'outil de protection des terminaux pour bloquer toute attaque future.

Échecs de connexion utilisateur

Insuffisances actuelles

Malgré la sophistication croissante des mesures de sécurité, les attaquants parviennent encore à compromettre des comptes par force brute et à en réinitialiser les mots de passe. Ce type d'attaque est difficile à contrer compte tenu du caractère anodin d'un tel comportement (les réinitialisations de mot de passe sont monnaie courante en entreprise). Il est donc essentiel d'entretenir une communication permanente entre les utilisateurs et les SOC pour établir une distinction entre activités normales et anormales.

Intérêt de l'orchestration

Un playbook d'orchestration de la sécurité peut être déclenché selon des paramètres définis par l'utilisateur (par exemple cinq échecs successifs de tentatives de connexion) et vérifier si l'activité est anodine ou malveillante.

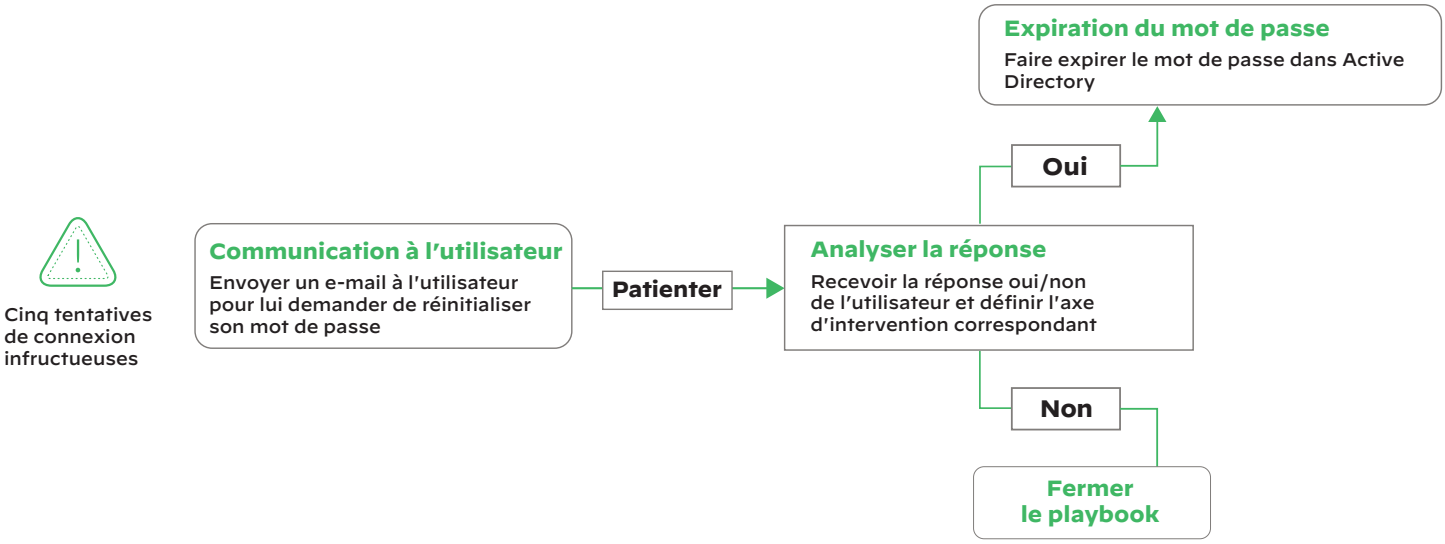

Figure 4 : Playbook d'échec de connexion utilisateur

Envoi d'e-mail

Le playbook envoie automatiquement à l'utilisateur concerné un e-mail qui l'informe de ses cinq tentatives d'authentification infructueuses et l'invite à confirmer qu'il en est bien à l'origine. L'e-mail demande à l'utilisateur de répondre par Oui ou par Non et explique l'action à entreprendre selon la réponse choisie.

Analyse de la réponse

Certaines plateformes d'orchestration peuvent analyser les réponses aux e-mails automatiques et exécuter différents axes d'intervention du playbook en conséquence.

Activité légitime

Si l'activité est légitime, le playbook réinitialise le mot de passe dans Active Directory® et envoie à l'utilisateur concerné un nouvel e-mail contenant ses nouveaux identifiants de connexion.

Activité malveillante

Si l'utilisateur répond qu'il n'est pas à l'origine de ces tentatives de connexion, le playbook envoie un nouvel e-mail qui l'informe d'une tentative de prise de contrôle de son compte. Le playbook peut également exécuter des actions d'investigation, comme l'extraction de l'adresse IP / l'origine géographique des tentatives ou la mise en quarantaine du terminal affecté.

Authentification depuis un lieu inhabituel

Insuffisances actuelles

Avec la mondialisation de l'économie, il est souvent difficile de distinguer une tentative d'accès VPN malveillante d'une connexion légitime par un collègue en déplacement dans un autre pays. Quant à l'adoption croissante du cloud, elle impose de vérifier les multiples sources de présence géographique, ce qui alourdit la charge de travail des équipes de sécurité tout en élargissant la surface d'attaque pour les cybercriminels.

Intérêt de l'orchestration

Certaines plateformes d'orchestration de la sécurité exécutent des playbooks non seulement dans le cadre de mesures réactives, mais aussi sous forme de workflows proactifs planifiés. Un playbook de contrôle VPN peut ainsi être planifié à intervalles réguliers pour identifier d'éventuelles anomalies VPN avant de les transmettre aux équipes de sécurité pour un examen plus approfondi.

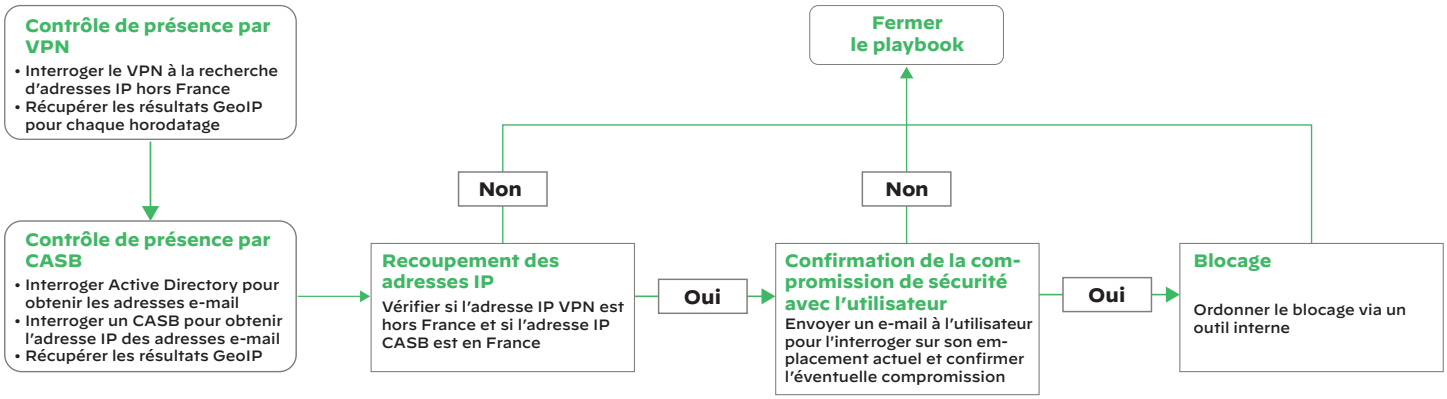

Figure 5 : Playbook de contrôle VPN

Contrôle de présence du VPN

Le playbook interroge le service VPN au sujet des adresses IP hors pays ou zones géographiques définies, puis récupère le résultat de recherche GeoIP pour chaque horodatage de ces adresses IP.

Contrôle de présence de CASB

Pour rapprocher les données VPN, le playbook interroge toutes les adresses e-mail d'Active Directory et les compare à un CASB (Cloud Access Security Broker) pour retrouver les adresses IP. Le playbook récupère ensuite les résultats GeoIP pour chaque horodatage de ces adresses IP.

Recoupement des adresses IP

Le playbook compare les adresses IP collectées par le service VPN à celles recueillies à partir du CASB. Lorsqu'il détecte une adresse IP VPN hors France associée à une adresse IP CASB en France, il envoie automatiquement un e-mail à l'utilisateur concerné pour qu'il confirme son emplacement actuel.

Réponse à une compromission de sécurité

Si l'utilisateur confirme qu'il s'agit bien d'une compromission, le playbook bloque l'adresse IP concernée au moyen d'outils internes et demande à un analyste sécurité de mener une investigation plus poussée.

Remarque : la condition décrite dans le playbook de la Figure 5 est fournie à titre d'illustration et peut être associée une multitude d'autres conditions pour les contrôles VPN. Par exemple, la condition « Déplacement impossible » peut être une condition par laquelle le playbook signale deux authentifications simultanées à partir de deux lieux distincts et déclenche une action.

Gestion des opérations de sécurité

Gestion des certificats SSL

Insuffisances actuelles

Souvent, les SOC sont tellement accaparés par la réponse à incident qu'ils n'ont que peu de temps à consacrer à la partie opérationnelle de leur rôle. Les certificats SSL périmés, les systèmes d'exploitation obsolètes et les failles non corrigées sur les terminaux sont autant de vulnérabilités qui laissent le champ libre à des attaques.

Intérêt de l'orchestration

Un playbook de gestion des certificats peut interroger tous les terminaux à intervalles réguliers pour détecter les certificats SSL sur le point d'expirer et prendre les mesures nécessaires.

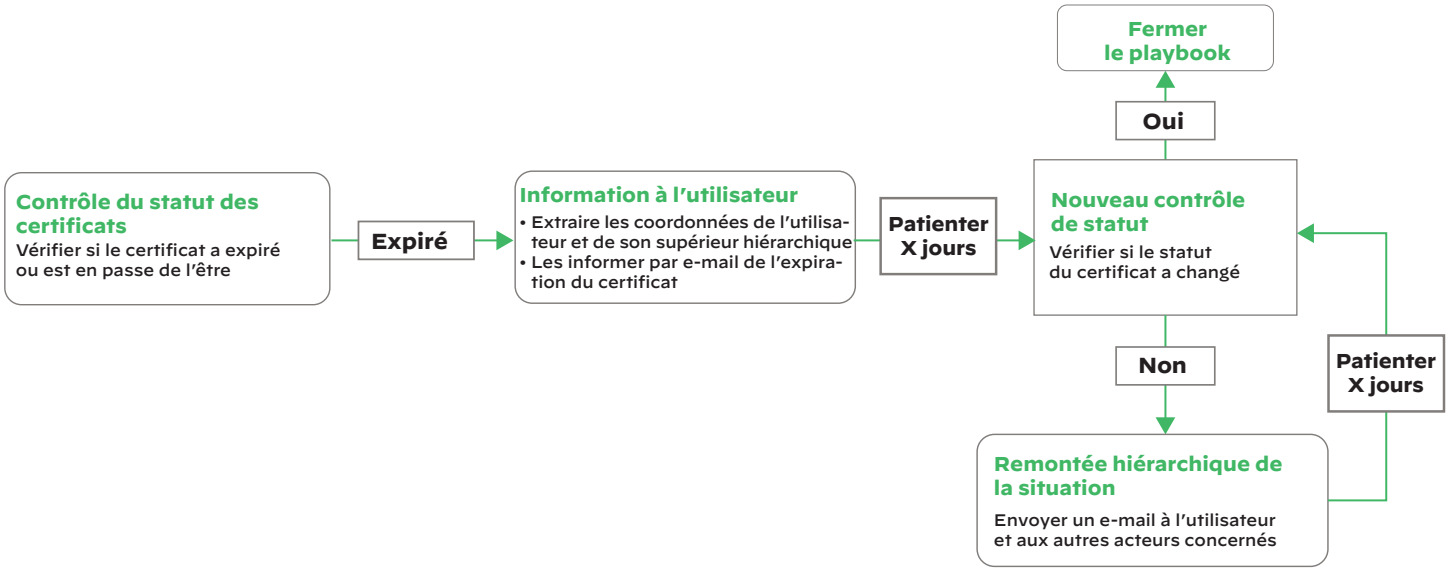

Figure 6 : Playbook de gestion des certificats SSL

Vérification du statut des certificats

Le playbook interroge un outil de gestion des certificats (par exemple Venafi®) pour recenser les terminaux dont les certificats SSL ont expiré ou arrivent à expiration.

Information à l'utilisateur

Lorsqu'il détecte des certificats problématiques, le playbook collecte les informations concernant l'utilisateur en question et son supérieur hiérarchique (à partir d'Active Directory, Salesforce®, etc.). Le playbook envoie ensuite automatiquement un e-mail à ces deux personnes pour leur signaler le certificat en question et les invitant à le renouveler.

Nouvelle vérification de statut

Le playbook vérifie une nouvelle fois le statut du certificat problématique quelques jours après l'envoi du premier e-mail.

Remontée hiérarchique

Si le certificat n'est toujours pas actualisé, le playbook envoie automatiquement un e-mail à l'utilisateur concerné, à son N+1 et aux autres administrateurs concernés pour porter la situation à leur attention.

Diagnostic des terminaux et démarrage des agents

Insuffisances actuelles

En termes de proactivité, les diagnostics et la maintenance des terminaux sont tout aussi importants que l'est leur protection en termes de réactivité. Les machines non gérées, dont les agents sont peu ou pas connectés ou dont les politiques de sécurité sont obsolètes, sont généralement des proies faciles pour les attaquants. Or, souvent, les équipes de sécurité sont trop occupées à répondre à des incidents pour pouvoir effectuer des diagnostics poussés sur les terminaux.

Intérêt de l'orchestration

Des playbooks peuvent être exécutés à intervalles réguliers pour réaliser des diagnostics sur tous les terminaux et assigner des techniciens à la correction de machines obsolètes.

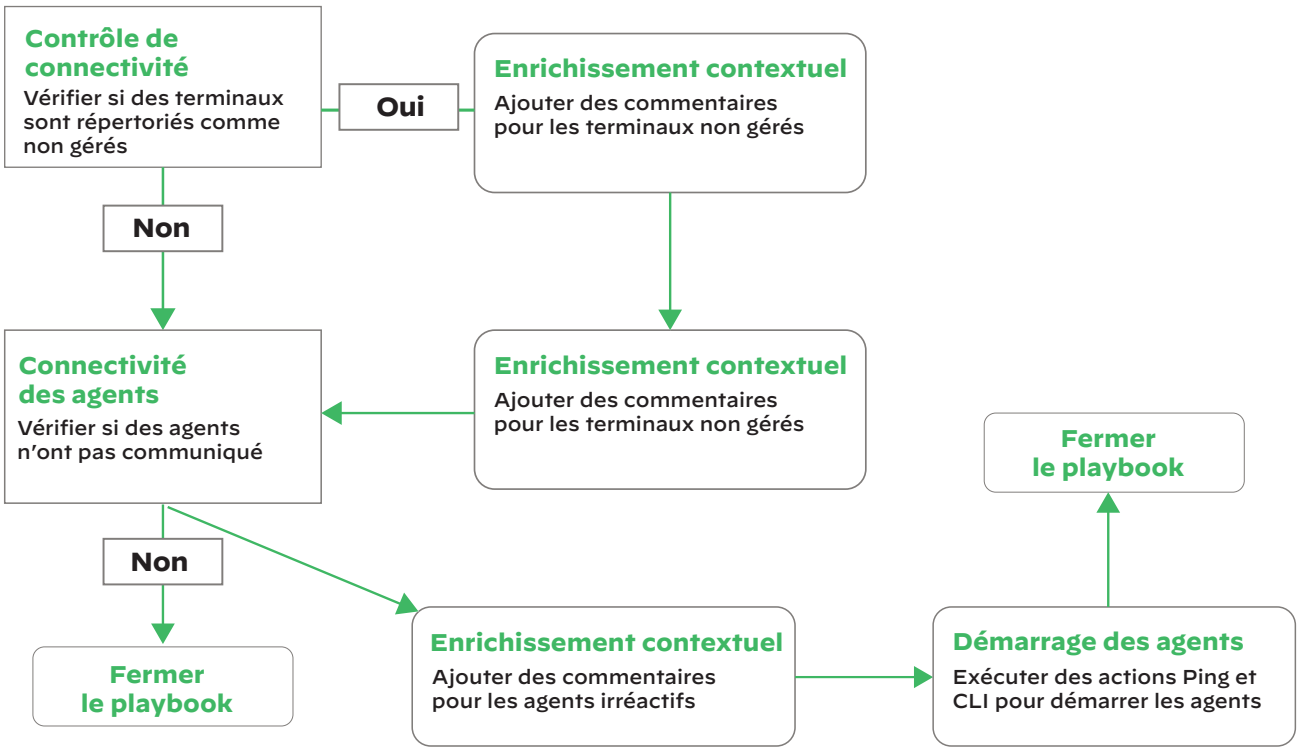

Figure 7 : Playbook de diagnostic des terminaux et de démarrage des agents

Vérification de connectivité

Le playbook fait appel à des outils comme McAfee ePO pour vérifier si certains terminaux apparaissent comme non gérés (sans agent). Dans l'affirmative, le playbook ajoute des commentaires à l'attention des analystes et crée un ticket pour faire remonter le problème.

Contrôle de connectivité des agents

Le playbook vérifie si des terminaux se trouvent hors du champ de communication des agents. Dans l'affirmative, il ajoute des commentaires à l'attention des analystes, crée un ticket et tente de démarrer des agents sur les terminaux concernés au moyen d'appels ping et d'autres méthodes.

Gestion des vulnérabilités

Insuffisances actuelles

La gestion des vulnérabilités est un processus d'importance stratégique qui couvre à la fois les dimensions proactive et réactive des opérations de sécurité. Comme cette pratique englobe toutes les ressources informatiques, les équipes de sécurité tentent souvent vainement de corréler des données entre les différents environnements. Elles passent alors beaucoup plus de temps à unifier ces informations qu'à corriger les vulnérabilités.

Intérêt de l'orchestration

Les playbooks d'orchestration de la sécurité peuvent automatiser l'enrichissement et la contextualisation des vulnérabilités avant de passer la main aux analystes pour une remédiation manuelle. Cette méthode permet de maintenir un équilibre entre les processus manuels et automatiques : les analystes évitent de gaspiller leur temps sur des tâches répétitives pour mieux se recentrer sur la prise de décisions essentielles et la rédaction de leurs conclusions.

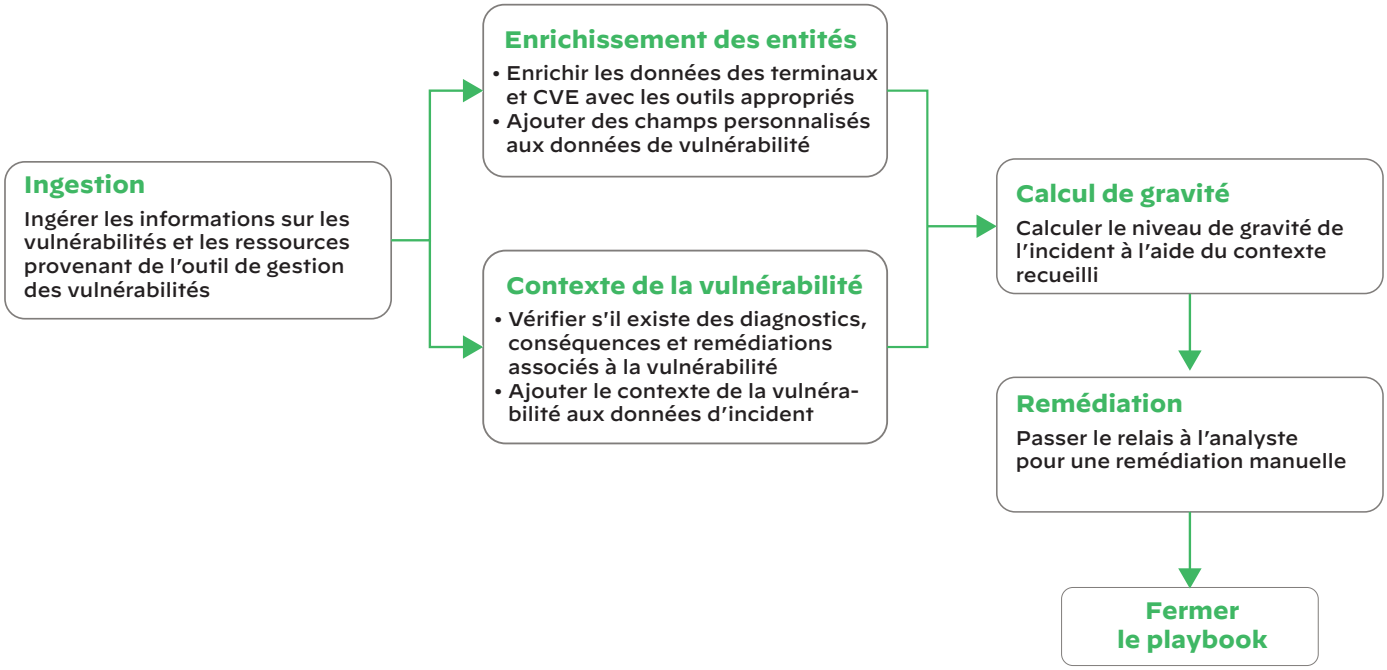

Figure 8 : Playbook de gestion des vulnérabilités

Ingestion

Le playbook ingère les informations sur les ressources et les vulnérabilités à partir d'un outil de gestion des vulnérabilités tel que Qualys®.

Enrichissement des entités

Le playbook enrichit les données des terminaux et des CVE (Common Vulnerabilities and Exposures) au moyen d'outils idoines. Il ajoute également des champs personnalisés à l'incident si les données ainsi recueillies l'exigent.

Contexte de la vulnérabilité

Le playbook interroge l'outil de gestion des vulnérabilités à propos des diagnostics, conséquences et remédiations liés à la vulnérabilité. Si des informations contextuelles sont découvertes concernant la vulnérabilité, elles sont ajoutées aux données de l'incident.

Calcul de gravité

En fonction des informations contextuelles recueillies, le playbook calcule le niveau de gravité de l'incident. Des informations complémentaires sur ce processus figurent dans le playbook d'attribution de niveaux de gravité, abordé plus loin dans ce livre blanc.

Remédiation

Le playbook passe le relais à un analyste de sécurité chargé d'investiguer et de corriger la vulnérabilité.

Traque des menaces et réponse à incident

Recherche rapide d'IoC

Insuffisances actuelles

Souvent trop occupées à gérer l'urgence au quotidien, les équipes de sécurité manquent de temps pour mener des opérations de traque et d'identification proactives des menaces à un stade précoce, avant qu'elles ne se manifestent dans les environnements utilisateurs. Et même lorsqu'elles parviennent à mener cette traque, la corrélation des flux de Threat Intelligence issus d'une multitude de sources s'opère souvent manuellement, laissant très peu de temps à la prise de décision.

Intérêt de l'orchestration

Les playbooks d'orchestration des réponses à incidents permettent de réaffecter les analystes à des tâches proactives comme la traque des menaces. Pour les exercices de traque proprement dits, les équipes de sécurité peuvent exécuter des playbooks qui ingèrent les IoC et recherchent des informations supplémentaires sur divers outils de Threat Intelligence.

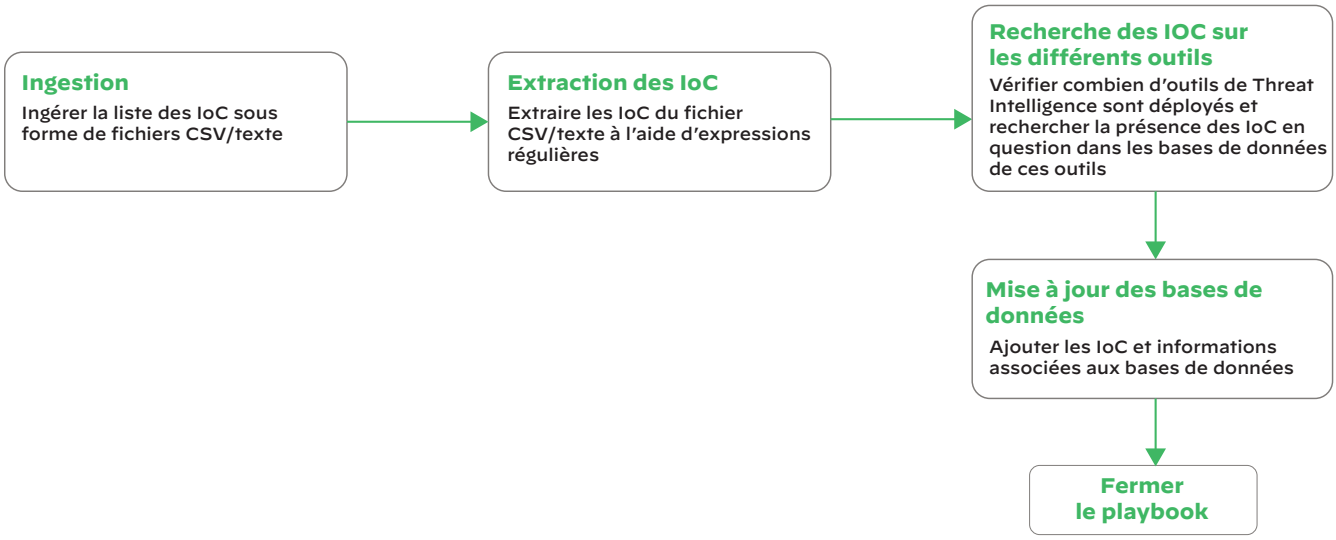

Figure 9 : Playbook de recherche rapide d'IoC

Ingestion

Le playbook ingère une liste d'IoC sous forme de fichiers CSV/texte.

Extraction des IoC

Le playbook ingère les IoC (adresses IP, URL, hachages, etc.) du fichier CSV/texte à l'aide d'expressions régulières, c'est-à-dire des modèles personnalisés prédéfinis.

Recherche des IoC sur les différents outils

Le playbook vérifie le nombre d'outils de Threat Intelligence déployés par le SOC et recherche les IoC extraits sur ces outils. Le cas échéant, le playbook contrôle également les terminaux pour vérifier si l'un d'eux a été compromis par les IoC en question.

Mise à jour des bases de données

Si un outil de Threat Intelligence détecte des IoC, le playbook actualise les bases de données des autres outils et listes noires en conséquence.

Analyse des malwares

Insuffisances actuelles

La détonation et l'analyse du comportement de fichiers suspects en sandbox est une étape cruciale et incontournable de tout exercice de réponse à incident. Les outils d'analyse de malware étant isolés des autres produits de sécurité, les analystes finissent par multiplier les allers-retours entre consoles, perdant ainsi un temps précieux. Un copier-coller des résultats sur une autre console demande également du temps et accroît le risque d'erreur.

Intérêt de l'orchestration

Les playbooks d'orchestration de la sécurité peuvent automatiser l'ensemble du processus de détonation des fichiers en sandbox, soit en tant que workflow isolé, soit en parallèle à d'autres activités d'enrichissement. Ainsi, les analystes ont accès aux résultats de l'analyse sans avoir à effectuer toute l'activité préparatoire en amont. Enfin, comme les playbooks consignent le résultat de toutes les actions sur une console centrale, plus besoin de saisir manuellement ces informations après les faits.

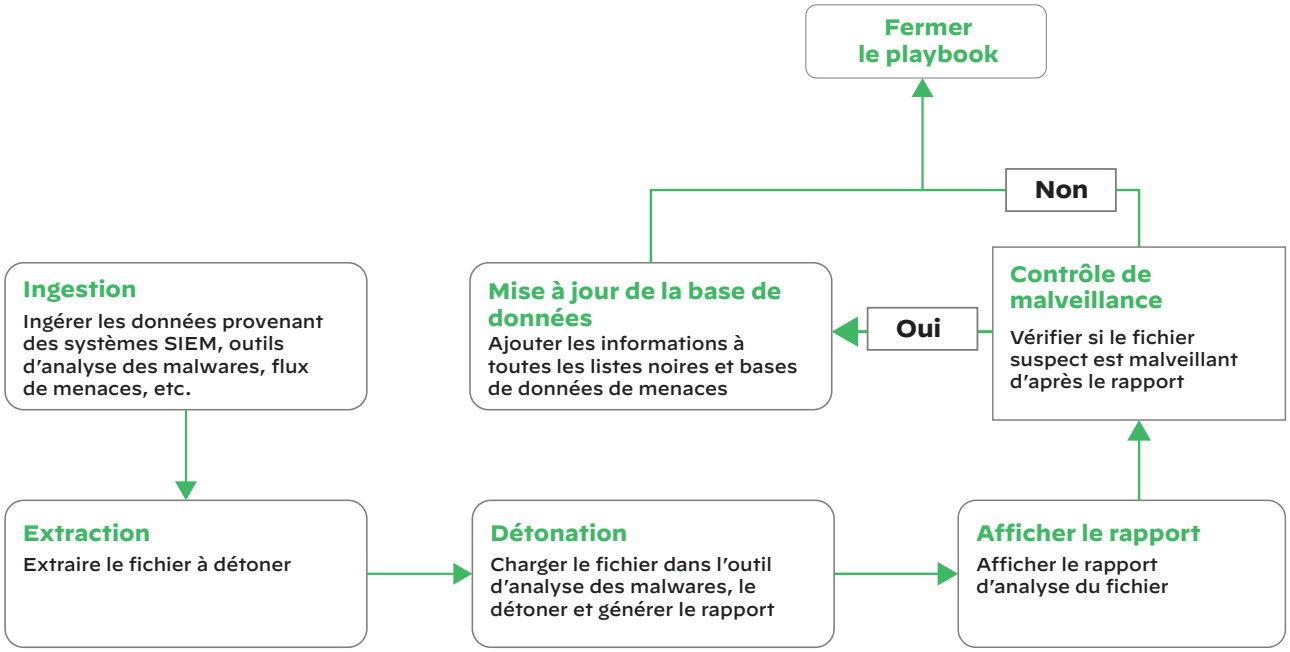

Figure 10 : Playbook d'analyse des malwares

Ingestion

Le playbook peut ingérer les données d'une variété de sources : systèmes SIEM, boîtes mail, flux de Threat Intelligence et outils d'analyse de malwares.

Extraction

Le playbook extrait le fichier à détoner.

Détonation

Le playbook charge le fichier dans l'outil d'analyse de malware, le détone et génère un rapport d'analyse.

Affichage du rapport

Le playbook affiche le rapport d'analyse afin que les analystes puissent l'étudier et engager les actions nécessaires.

Mise à jour de la base de données

Si la nocivité du fichier est avérée, le playbook ajoute ces informations aux listes noires concernées. De là, le playbook peut déclencher d'autres actions, telles que la mise en quarantaine des terminaux infectés, la création de tickets et le recoupement de données issues d'autres flux de Threat Intelligence.

Réponse à incident orientée cloud

Insuffisances actuelles

Du point de vue de la réponse à incident, les données et processus de sécurité dans le cloud sont souvent séparés des mesures de sécurité traditionnelles, exigeant de ce fait plusieurs consoles pour gérer le dispositif de sécurité dans son ensemble. En termes opérationnels, la gestion des identifiants de service est une tâche fastidieuse, car chaque service est associé à une clé ou un mot de passe pour appeler différents ensembles d'API.

Intérêt de l'orchestration

Les playbooks d'orchestration de la sécurité peuvent unifier les processus des infrastructures de sécurité sur site et dans le cloud. Les équipes de sécurité peuvent alors piloter la réponse à incident depuis une seule et même console. Certaines plateformes d'orchestration s'intègrent également aux outils de gestion d'identité dans le cloud, permettant ainsi de déployer des services basés sur les rôles, sans clé et sans gestion d'identifiants.

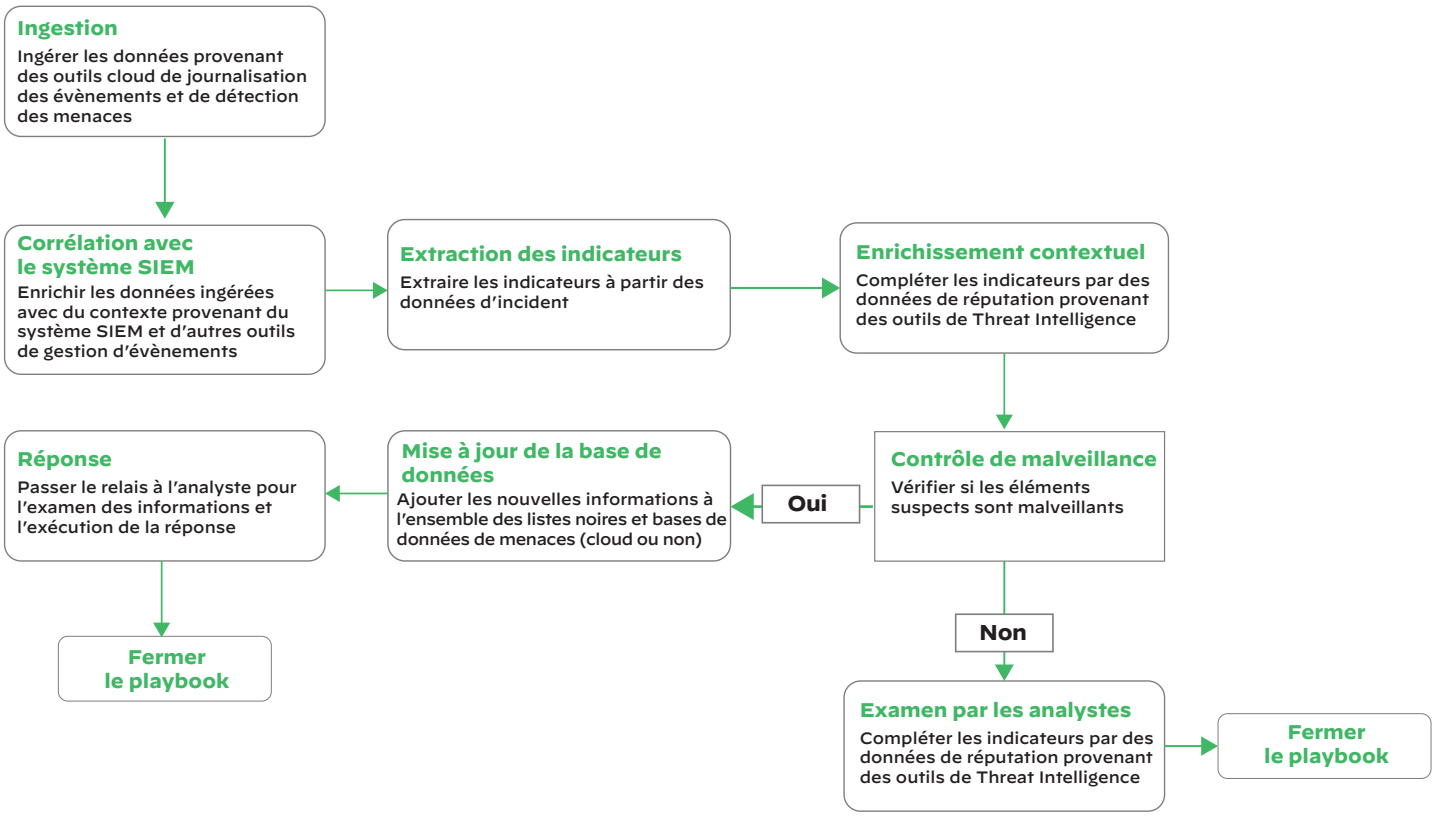

Figure 11 : Playbook de réponse à incident orientée cloud

Ingestion

Le playbook ingère les données issues d'outils cloud de journalisation des évènements et de détection des menaces, comme Amazon GuardDuty® ou Amazon CloudWatch.

Corrélation avec le système SIEM

Le playbook contextualise les données ingérées au moyen de systèmes SIEM et d'autres outils non cloud de gestion des évènements pour mesurer la portée totale de l'attaque présumée.

Extraction des indicateurs

Le playbook extrait les indicateurs (adresses IP, URL, hachages, etc.) des données d'incident.

Enrichissement

Le playbook complète les indicateurs par des données de réputation provenant des outils de Threat Intelligence utilisés par le SOC.

Vérification de malveillance

Le playbook vérifie si les indicateurs sont identifiés comme malveillants. Dans l'affirmative, il actualise les bases de données et les listes noires (dans le cloud ou non) avant de passer la main à un analyste de sécurité pour une analyse plus approfondie. Si les indicateurs ne sont pas identifiés comme malveillants, le playbook demande à un analyste sécurité d'examiner les informations et de vérifier l'absence de risque avant de clore l'incident.

Automatisation de sécurité adaptable

Enrichissement contextuel des IoC

Insuffisances actuelles

L'enrichissement contextuel des indicateurs de compromission est l'une des premières tâches que réalisent les équipes de sécurité lorsqu'elles répondent à un incident. La problématique ici est double. D'abord, ce processus d'enrichissement des indicateurs est aussi répétitif qu'il est important. Les analystes risquent donc de s'enliser dans ce travail fastidieux alors que l'attaque gagne du terrain. Ensuite, le cloisonnement des outils de sécurité entrave le rapprochement des données de Threat Intelligence entre les différentes plateformes. Il devient alors difficile de rendre un verdict sur le caractère éventuellement malveillant des indicateurs observés.

Intérêt de l'orchestration

Les playbooks d'orchestration de la sécurité peuvent automatiser l'enrichissement contextuel des indicateurs en interrogeant plusieurs outils de Threat Intelligence. En exécutant ce playbook au début de la réponse à incident, les équipes de sécurité disposent en quelques secondes du contexte nécessaire pour engager leurs investigations.

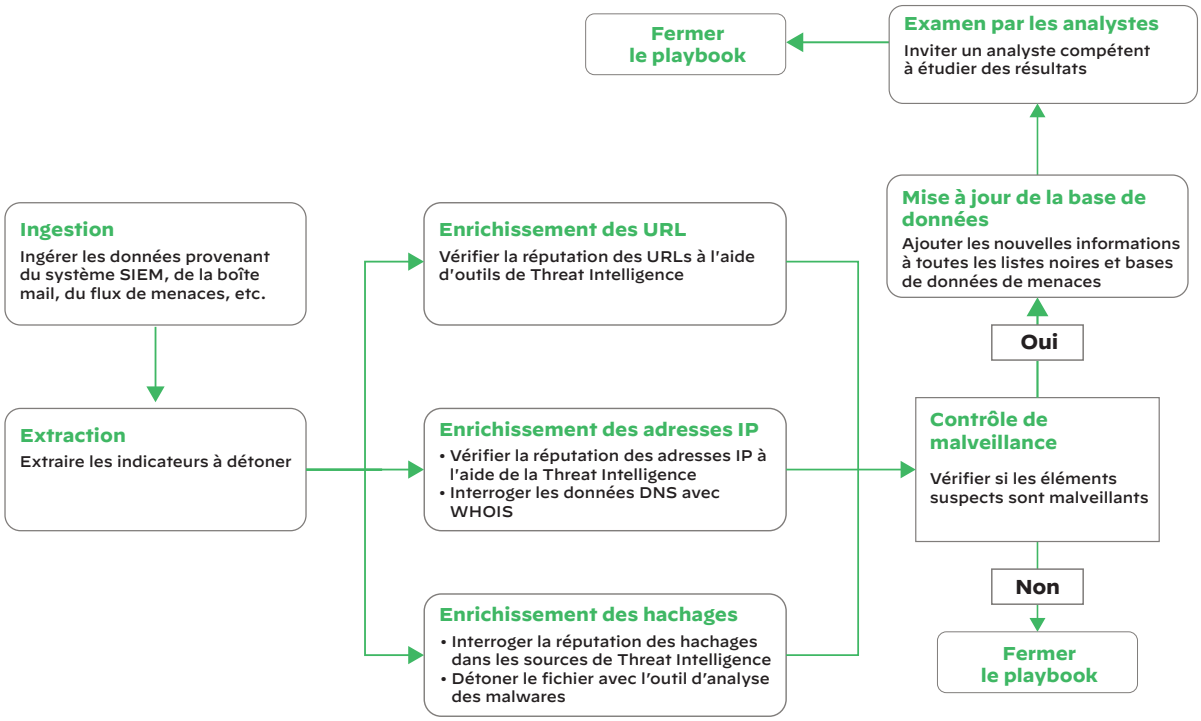

Figure 12 : Playbook d'enrichissement contextuel des IoC

Ingestion

Le playbook peut ingérer les données d'une variété de sources, telles que les systèmes SIEM, boîtes mail et flux de Threat Intelligence.

Extraction

Le playbook extrait les IoC (adresses IP, URL, hachages, etc.) à enrichir.

Enrichissement contextuel des données

Le playbook enrichit les IoC à partir de tous les outils de Threat Intelligence exploités par le SOC. Par exemple, les URL sont contextuellement enrichies par des outils comme Cofense® et CrowdStrike Falcon® Intel, les adresses IP par des outils de Threat Intelligence et des services DNS tels que WHOIS, et les hachages par des outils de Threat Intelligence et d'analyse de malware tels que le service de prévention des malwares Palo Alto Networks WildFire®.

Mise à jour des bases de données

Le playbook exécute les actions initiales de réponse en fonction du caractère malveillant des éléments détectés. Si celui-ci est avéré, les éléments en question sont intégrés aux référentiels de Threat Intelligence et aux listes noires des outils pour prévenir toute future attaque utilisant les mêmes techniques.

Examen par des analystes

Le playbook vérifie si les indicateurs sont identifiés comme malveillants. Dans l'affirmative, le playbook relève le niveau de gravité de l'incident, ouvre un ticket et demande à un analyste compétent d'approfondir l'investigation. Dans la négative, le playbook enregistre le contexte pour référence ultérieure et clôt l'incident, évitant ainsi aux analystes de perdre leur temps sur des faux positifs.

Attribution d'un niveau de gravité aux incidents

Insuffisances actuelles

À l'heure où l'arsenal des produits de sécurité du SOC est en pleine expansion, chacun de ces outils envoie ses propres alertes, d'où de nombreux doublons que les analystes de sécurité doivent trier. Par ailleurs, les disparités dans le paramétrage de sensibilité des produits posent problème. Si un déclencheur d'alerte n'est pas assez sensible, des incidents dangereux peuvent passer à travers les mailles du filet et causer un préjudice réel pour l'entreprise. S'il est trop sensible, les analystes reçoivent d'innombrables faux positifs qui causent autant de pertes de temps que de frustrations.

Intérêt de l'orchestration

Lorsqu'un incident est ingéré dans la plateforme d'orchestration, un « playbook de notation du niveau de gravité » peut analyser tous les ensembles de données pour définir le niveau de gravité de l'incident et y attribuer un niveau de priorité approprié. Les analystes peuvent alors traiter en priorité les incidents les plus critiques.

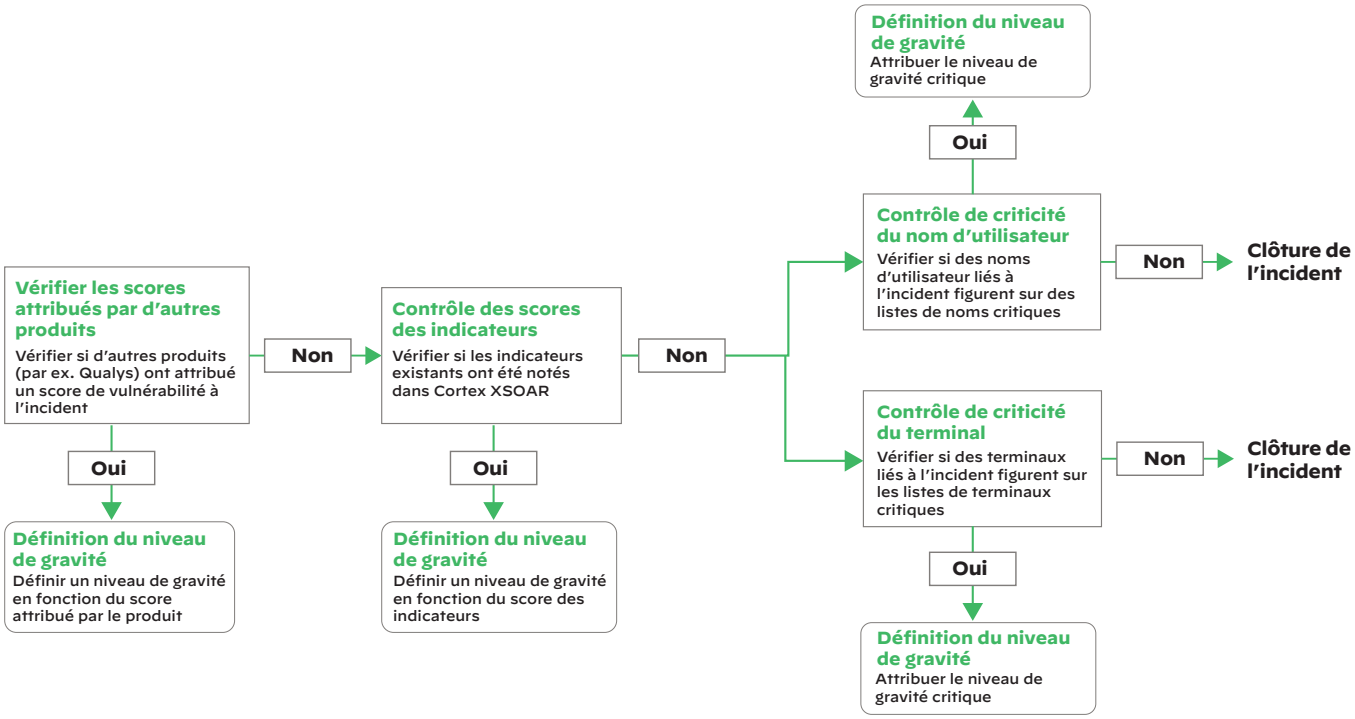

Figure 13 : Playbook de notation du niveau de gravité des incidents

Recherche de scores sur les produits externes

Le playbook vérifie d'abord si un produit externe de gestion des vulnérabilités a enregistré un niveau de gravité pour l'incident en question. Par exemple, le playbook peut interroger Qualys pour vérifier s'il existe un enregistrement du niveau de gravité, puis attribuer le même score à l'incident dans la plateforme d'orchestration.

Ces actions permettent aux équipes d'exploiter les atouts de leurs produits de sécurité (comme la notation des niveaux de gravité dans Qualys), évitant ainsi de jongler entre les écrans pour exécuter manuellement des tâches triviales.

Contrôle des scores des indicateurs

En l'absence d'informations tierces sur le niveau de gravité, le playbook passe en revue les indicateurs (adresses IP, URL, hachages de fichier) de l'incident et vérifie l'existence éventuelle d'un « score de menace » associé à tel ou tel indicateur.

Remarque

Certaines plateformes d'orchestration enregistrent automatiquement tous les indicateurs ingérés dans le cadre d'incidents, puis attribue à chacun une « réputation » sur la base d'un recoupement de scores attribués par d'autres plateformes de Threat Intelligence auxquelles le SOC s'intègre.

S'il existe un score associé à un indicateur, le playbook le prend en compte pour attribuer un niveau de gravité élevé, moyen ou faible. Si le SOC s'intègre à de multiples produits de Threat Intelligence, il peut capitaliser sur les analyses de chaque produit pour établir un score consolidé.

Contrôle des entités critiques

Outre la Threat Intelligence, le playbook doit également prendre en compte l'identité et le comportement des utilisateurs lorsqu'il attribue un niveau de gravité à l'incident. Le playbook vérifie s'il existe un nom d'utilisateur associé à l'incident et s'il appartient à une liste d'utilisateurs critiques. Il réalise ces mêmes contrôles avec le nom d'hôte associé à l'incident. Si le nom d'utilisateur ou le nom d'hôte exige une réponse prioritaire, le playbook attribue à l'incident un niveau de gravité « critique ».

CORTEX
BY PALO ALTO NETWORKS

Vous souhaitez en savoir plus sur l'orchestration ?

Téléchargez gratuitement Cortex XSOAR Community Edition

Essai gratuit

Rapport 2019 sur l'état du SOAR

Télécharger le rapport

paloalto NETWORKS

Oval Tower, De Entrée 99-197,
1101HE Amsterdam,
Pays-Bas

+31 20 888 1883

www.paloaltonetworks.fr

top-security-orchestration-use-cases-wp-100220-fr