LIVRE BLANC

Éliminez les angles morts et boostez votre centre d'exploitation de sécurité (SOC) grâce aux informations de Symantec® Threat Hunter

Symantec by Broadcom

SOMMAIRE

En bref

Les trois ingrédients essentiels pour une détection et une intervention rapides en cas d'incident :

- Données, tant au niveau de l'entreprise qu'à l'échelle planétaire.
- Intelligence artificielle, pour traiter les énormes volumes de données.
- Chercheurs et experts en menaces, pour identifier les tentatives de reconnaissance avant que la violation ne se fasse jour.

Threat Hunter est une nouvelle fonction de Symantec® Endpoint Security Complete (SESC) qui rassemble ces trois ingrédients essentiels pour permettre aux équipes de sécurité d'intervenir rapidement en cas d'incident et de mettre un terme aux violations.

Nos analystes en cybermenaces de renommée mondiale sont les mêmes que ceux qui ont découvert Stuxnet et WastedLocker. Ils analysent les informations de Machine Learning issues des données télémétriques mondiales des clients. Ils fournissent aux entreprises des informations essentielles par le biais de la console produit SESC afin de renseigner les équipes du centre d'exploitation de sécurité (SOC) des tentatives de violation potentielles.

Ces informations peuvent inclure les détails de campagne, outils, tactiques et procédures utilisés par les pirates, ainsi que des conseils sur la façon de réagir. Les équipes SOC peuvent tirer parti des informations sur les incidents ayant fait l'objet d'un examen manuel pour prendre les mesures appropriées à l'aide du vaste kit d'outils SESC. Ces mesures peuvent impliquer notamment la mise en quarantaine d'appareils, l'application de politiques pour autoriser ou bloquer des applications ou encore l'interdiction de comportements indésirables d'applications légitimes.

« Ce qui différencie Threat Hunter d'un service géré, c'est que nous n'essayons pas de remplacer le centre d'exploitation de sécurité du client, ni de gérer tout son environnement. Le but est d'affiner les compétences des employés en fournissant un maximum d'informations et en les rendant exploitables afin que le client puisse réagir rapidement. Cette fonction doit être considérée comme une deuxième paire d'yeux, un moyen de débusquer les attaques critiques qui auraient pu passer inaperçues étant donné que le personnel du SOC se consacrait à d'autres priorités. »

Introduction

Pour lutter contre les menaces sophistiquées qui pèsent aujourd'hui sur les entreprises, les plates-formes Endpoint Protection et les solutions Endpoint Detection and Response (EDR) ne suffisent plus. Les entreprises ont besoin de nouveaux outils pour éliminer les angles morts et déjouer les tactiques et techniques mises en œuvre par les pirates informatiques et contre lesquelles les outils traditionnels sont impuissants. Parmi les angles morts les plus courants se trouvent les signes non détectés d'une violation. Les membres d'une équipe SOC disposent généralement de toute une panoplie d'outils pour détecter une menace. Cependant, ils sont souvent submergés par les volumes de données à traiter. Plus important encore, il leur manque les ressources nécessaires pour investiguer chaque alerte et détecter les attaques ciblées de grande envergure.

SESC fournit le contexte adéquat avec sa fonction Threat Hunter.

Repenser la détection des violations avec Symantec Threat Hunter

Les outils et techniques traditionnels de détection des violations peuvent facilement passer à côté des menaces les plus dangereuses qui pèsent sur l'entreprise. En règle générale, ils ne capturent que des analyses isolées provenant de points de terminaison à l'échelle de l'entreprise, tels que des terminaux, des systèmes de messagerie, des proxys, etc. Étant donné que cette approche ne permet pas d'avoir une vision globale des nouvelles menaces, les équipes de sécurité doivent corréler manuellement ces analyses et les intégrer dans des renseignements limités sur les menaces émanant de sources externes. De plus, la plupart des entreprises ne disposent pas des compétences nécessaires pour concevoir des algorithmes d'intelligence artificielle, ni de chercheurs qualifiés pour examiner les groupes d'attaques. Cela se traduit par un manque de visibilité des menaces, des détections moins précises et des temps d'arrêt plus longs.

Threat Hunter offre aux équipes de sécurité la possibilité de réagir rapidement aux incidents qui touchent les terminaux et d'atténuer l'impact des attaques. Réduction de la surface d'attaque, prévention des attaques, prévention des violations, détection et réponse… Cette fonction centrale de SESC intègre les technologies nécessaires pour assurer une protection totale sur toute la chaîne d'attaque. Threat Hunter allie de précieuses données télémétriques, les technologies de machine learning et des recherches sur les menaces menées par les meilleurs experts du secteur pour offrir aux équipes SOC des notifications d'incidents personnalisées et classées par priorité, ainsi que des recommandations d'intervention.

Threat Hunter se distingue des solutions de détection et de réponse gérées traditionnelles en ce sens que l'équipe Symantec Enterprise Division ne remplace pas l'équipe SOC, mais lui fournit des informations, plutôt que d'assurer une surveillance tactique des événements. Cela fait des années que les chasseurs de menaces, ou Threat Hunters, de Symantec sont à la pointe de la recherche. Véritables limiers de la sécurité informatique, ils identifient les formes de menaces avancées les plus difficiles à saisir. Parfaitement au fait des outils, tactiques et procédures utilisés par les pirates informatiques, ils sont capables de déceler les indices les plus infimes et de dresser un tableau de l'attaque en cours au sein de votre entreprise. Ils savent comment y répondre et ils peuvent vous guider.

Symantec Threat Hunter arrête le ransomware WastedLocker

Evil Corp n'est pas seulement une société fictive issue d'une série télévisée. C'est aussi un gang de cybercriminels bien réel qui continue de sévir malgré les mises en accusation de ses dirigeants par le FBI. En juin 2020, Evil Corp a lancé une attaque par ransomware ciblée baptisée WastedLocker contre quelques-unes des principales entreprises américaines. Cette attaque aurait facilement pu les mettre toutes KO.

L'attaque était dirigée principalement contre des grandes entreprises, dont huit figurent dans le classement Fortune 500. À l'exception de la filiale américaine d'une multinationale étrangère, toutes les entreprises ciblées étaient américaines. L'objectif de ces attaques était de paralyser l'infrastructure informatique des victimes en chiffrant la plupart des ordinateurs et serveurs afin d'exiger une rançon de plusieurs millions de dollars.

Découverte et conclusions

La compromission initiale concernait le framework SocGholish, distribué à la victime sous la forme d'un fichier JavaScript zippé se faisant passer pour une mise à jour de navigateur sur des sites web légitimes compromis. Un deuxième fichier JavaScript profilait l'ordinateur à l'aide de commandes telles que whoami, net user et net group. Il utilisait ensuite PowerShell pour télécharger d'autres scripts PowerShell liés à la découverte. Une fois qu'ils avaient accès au réseau de la victime, les pirates utilisaient Cobalt Strike parallèlement à plusieurs outils déjà présents dans l'environnement (« Living-off-the-Land ») pour voler les informations d'authentification et déployer le ransomware WastedLocker sur plusieurs ordinateurs du réseau.

Les attaques ont été détectées de manière proactive sur un certain nombre de réseaux par l'analytique des attaques ciblées sur le cloud de Symantec. Après examen, l'équipe Threat Hunter de Symantec a vite compris que l'activité correspondait étroitement à une activité bien documentée, observée dans les premiers stades des attaques WastedLocker.

Intervention de l'équipe Threat Hunter

Cette découverte a permis à l'équipe Threat Hunter de Symantec d'identifier d'autres entreprises ciblées par WastedLocker, ainsi que d'autres outils, tactiques et procédures utilisés par les pirates. Grâce à ces informations, les analystes de Symantec ont pu renforcer les mesures de protection de Symantec à tous les stades de l'attaque. Dans le même temps, l'équipe a averti 68 clients que des pirates avaient infiltré leurs réseaux et préparaient le terrain pour lancer des attaques par ransomware. Ces avertissements proactifs par téléphone et courrier électronique ont permis à l'équipe de contrecarrer les attaques. Si les attaques avaient abouti, les dommages auraient pu se chiffrer en millions de dollars et cela aurait pu avoir un effet domino sur les chaînes d'approvisionnement.

Défis pour les équipes du centre d'exploitation de sécurité

Plus la détection d'un incident est précoce, plus il est facile d'y remédier. Cependant, les équipes de sécurité doivent relever de nombreux défis lorsqu'elles tentent de détecter une attaque sophistiquée et d'en révéler toute l'étendue. Lassitude vis-à-vis des alertes, problèmes de dotation en personnel, nécessité de disposer d'un filet de sécurité et d'informations contextuelles plus approfondies… Les difficultés ne manquent pas !

Lassitude vis-à-vis des alertes en raison des faux positifs

Les outils de sécurité génèrent énormément d'alertes, créant une situation où la quantité l'emporte sur la qualité. Les analystes en sécurité peuvent ainsi recevoir jusqu'à 10 000 alertes par jour. Pour les traiter, les analystes SOC doivent examiner chaque alerte afin d'en déterminer la validité. Cependant, le nombre élevé de faux positifs rend leur tâche encore plus fastidieuse. Un nombre sans cesse croissant d'alertes doivent être triées, suivies et validées. Ce processus éprouvant génère du stress et surcharge considérablement les équipes de sécurité. Par conséquent, les alertes critiques peuvent facilement passer entre les mailles du filet.

Une étude réalisée par Enterprise Strategy Group sur le lien entre la maturité de la sécurité et le « business enablement » fait apparaître qu'en mars 2020, près de deux-tiers des entreprises de premier plan ignoraient 25 % de leurs événements et alertes de sécurité, car il s'avère *difficilement réalisable* de se consacrer à chaque alerte en particulier (Enterprise Strategy Group, The Relationship Between Security Maturity and Business Enablement [5 mai 2020]). Une étude menée par le Ponemon Institute révèle, en outre, que le temps moyen d'identification d'une violation est de 197 jours ; le temps moyen pour contenir un incident de sécurité étant de 69 jours (Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview [Juillet 2018]). À l'évidence, les équipes SOC ont besoin d'une méthode permettant de raccourcir les temps de détection et de confinement, et de remédier aux alertes non traitées.

Selon une croyance bien ancrée, la corrélation des alertes permettrait de résoudre le problème lié à leur surcharge. En réalité, ni la corrélation ni le filtrage ne sont des opérations simples. Ce qu'il faut, ce sont des compétences humaines et des algorithmes créés par des experts.

De la nécessité d'avoir plus de contexte
Dans le cas d'une alerte, les analystes SOC ont besoin de tous les détails concernant l'attaque et son auteur afin de se concentrer sur la détection et la résolution. Malheureusement, à moins d'avoir une connaissance approfondie des indicateurs de compromission (IOC) d'une attaque et des noms de signatures, il peut s'avérer difficile d'identifier les indicateurs qui sont peut-être passés inaperçus et de déterminer quels événements discrets sont liés, et ceux qui ne le sont pas.

Les équipes de sécurité doivent savoir si une alerte est sérieuse, et elles ont besoin d'indices pour déterminer comment l'attaque est menée et quelle partie de l'entreprise est ciblée. Elles doivent aussi tout savoir des cybercriminels, ainsi que de leurs tactiques, techniques et procédures, pour déterminer au mieux comment les empêcher d'accéder aux réseaux et aux ressources.

Problèmes de dotation en personnel et nécessité de disposer d'un filet de sécurité
Compte tenu de la surcharge de menaces et du rythme de travail effréné des analystes en charge de la protection de l'entreprise, le risque de passer à côté d'une alerte en raison d'un manque de personnel est réel, ce qui n'est pas sans conséquences pour l'entreprise. Selon un rapport de recherche d'avril 2019 du Ponemon Institute, le coût moyen d'une violation de données est de 3,92 millions de dollars (Ponemon Institute, Cost of a Data Breach Report 2019 [Avril 2019]). Si une menace passe à travers les mailles du filet, les équipes SOC internes doivent avoir l'assurance qu'une autre équipe d'analystes qualifiés disposant d'outils efficaces se tient prête à l'intercepter.

Analyse des données de Threat Hunter

Threat Hunter combine des informations de télémétrie locales et mondiales, l'analyse des données de Machine Learning, et des données d'analyse examinées et validées manuellement par les chasseurs de menaces spécialisés de Symantec pour exposer les menaces qui, autrement, auraient échappé à la détection.

Vaste ensemble de données de télémétrie locales et mondiales
Threat Hunter repose sur un vaste ensemble de données mondiales pour effectuer ses analyses. Notre lac de données de référence collecte des données d'événement en provenance de tous les produits du portefeuille Symantec, y compris les applications pour le cloud, la messagerie, les réseaux et les terminaux. Threat Hunter recueille également des informations sur les menaces que d'autres clients ont pu rencontrer afin d'offrir une vision vraiment globale. Cet immense ensemble de données permet à Threat Hunter de gagner en capacité d'analyse et de continuer à s'améliorer à mesure que de nouvelles données sont reçues.

« C'est le sentiment de sécurité que vous ressentez lorsque quelqu'un de bienveillant regarde par-dessus votre épaule. Même les entreprises bien établies qui possèdent leurs propres équipes de lutte contre les menaces peuvent bénéficier de ce filet de sécurité, dans la mesure où nous envisageons les choses sous un autre angle. Nous ne nous limitons pas aux données d'un seul client, mais nous adoptons une approche globale. En détectant la même attaque sur d'autre réseaux, nous sommes en mesure de lancer des avertissements précoces aux clients qui ont peut-être été touchés, mais n'ont pas encore décelé les signes annonciateurs de l'attaque. Ainsi, il se peut qu'une équipe SOC ne détecte que les trois premières phases d'activité d'un pirate informatique. Cependant, grâce à notre vision globale, nous connaissons les trois phases suivantes. En fournissant ces informations globales, Threat Hunter donne à l'équipe SOC les moyens d'identifier ces phases et d'empêcher leur déclenchement. »

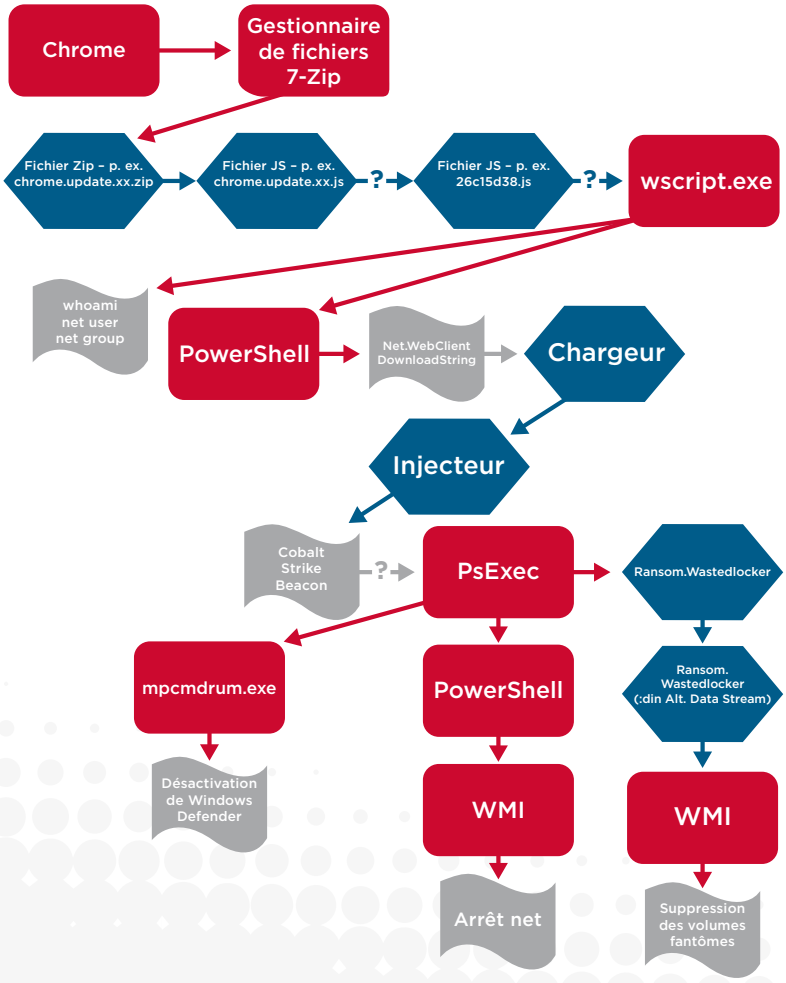
« Ce qui différencie véritablement Threat Hunter d'une équipe de lutte contre les menaces interne, c'est l'accès à l'ensemble des données de télémétrie de Symantec. Cela comprend le courrier électronique, le réseau, le cloud, ainsi que d'autres sources de données. Nous pouvons utiliser ces informations pour remonter jusqu'à la source de la menace, vérifier que l'attaque est bien réelle et obtenir davantage de contexte. Dans le cas d'un malware, par exemple, le fait que nous disposions des données de messagerie nous permet de remonter jusqu'à un fichier malveillant qui a été distribué dans un courrier spécifique. »

Analytique des attaques ciblées

L'analyse des données de Threat Hunter repose sur l'analytique des attaques ciblées, ce qui comprend les applications analytiques pour détecter les violations, PowerShell, les techniques de mouvement latéral, et les activités de balisage de commande et de contrôle. Ce type d'analytique a recours à l'Advanced Machine Learning et à l'intelligence artificielle basée sur le cloud pour passer au crible le lac de données en vue d'identifier les incidents et d'effectuer des analyses évolutives. Les experts en science des données s'appuient sur de solides compétences pour développer de nouveaux algorithmes d'intelligence artificielle exécutés sur ce lac de données. De plus, les analystes en sécurité évaluent les informations et fournissent des commentaires. Ce réentraînement humain des algorithmes affine le moteur analytique afin de limiter le nombre de faux positifs et de renforcer la précision des alertes.

Lorsque les algorithmes détectent une activité suspecte, l'équipe de recherche de Threat Hunter l'examine et joint à l'alerte des informations détaillées sur les tactiques, techniques et procédures employées par les pirates afin de contextualiser l'attaque et de permettre aux analystes SOC d'identifier rapidement la menace. Reportez-vous à l'illustration suivante.

Illustration 1 : Threat Hunter permet de retracer les étapes intermédiaires entre l'intrusion et le point de déclenchement d'une attaque. En même temps, l'analytique des attaques ciblées Threat Hunter et les analystes peuvent repérer une activité malveillante en n'importe quel point, ce qui améliore sensiblement la capacité du client à détecter et éradiquer rapidement la menace.



« Le contexte fourni par Threat Hunter est important, surtout lorsque des parties du réseau ne sont pas visibles par Symantec. Lorsque nous fournissons du contexte sur un cheval de Troie que nous avons détecté sur un ordinateur, ces analystes SOC sont en mesure d'associer ces informations à une liste plus étoffée d'IOC et de les appliquer aux parties du réseau sur lesquelles la visibilité est insuffisante. Cela constitue une énorme valeur ajoutée par rapport au client d'un terminal qui n'a peut-être pas prêté attention à la détection d'un cheval de Troie et qui ne communique en aucune façon avec Symantec. »

L'équipe Symantec Threat Hunter
L'équipe Symantec Threat Hunter est la mieux placée pour traiter la problématique des angles morts. Nos analystes jettent un œil avisé sur les incidents critiques et configurent des notifications à l'intérieur du produit SESC lorsque la menace point à l'horizon ou lorsque le pirate commet son méfait. Ce faisant, ils attirent l'attention des équipes SOC sur les zones sur lesquelles elles doivent concentrer leurs efforts.

Cela fait des années que les analystes de l'équipe Threat Hunter sont à la pointe de la recherche dans le domaine de la sécurité. De plus, ils cumulent des décennies d'expérience avec les données globales de Symantec. Cette expérience est encore renforcée par une grande expertise sectorielle et des compétences techniques en matière de création d'outils pour mieux comprendre le contexte des menaces. Cet ensemble de talents leur permet d'avoir une vision globale de l'évolution des menaces, tactiques et techniques en dehors de l'environnement SOC.

Collaborer pour garantir une réponse rapide et efficace

La puissance collective des produits de la gamme Symantec vient enrichir chaque donnée saisie par les membres de l'équipe Threat Hunter. Lorsqu'une attaque est découverte, les analystes de l'équipe Threat Hunter collaborent avec l'équipe Symantec Security Response pour l'analyser, s'assurer que des mécanismes de protection sont en place et en identifier la nature. Symantec Security Response s'emploie à améliorer les mesures de protection existantes et, le cas échéant, à créer des contrôles supplémentaires. Ces nouvelles mesures sont distribuées à l'échelle de l'entreprise pour bloquer l'attaque. Les autres clients en profitent également. Ils sont peut-être touchés par la même menace, mais ils n'en ont pas encore décelé les signes. La nouvelle mesure de protection est distribuée à l'ensemble de la communauté des clients Symantec en vue d'une mise en œuvre globale.

Les enquêtes sur les menaces réalisées par le biais de Threat Hunter s'inscrivent dans un processus dit « detect-to-prevent » (détecter pour protéger) dans lequel les détections passées conduisent à une stratégie de prévention plus robuste. En établissant un lien avec les alertes déclenchées par un comportement malveillant et en adaptant les politiques d'isolement associées, les analystes SOC peuvent utiliser chaque enquête pour véritablement améliorer leur stratégie de sécurité des terminaux au fil du temps. Notre solution Endpoint Detection and Response (EDR) et de prévention entièrement intégrée garantit aux analystes SOC une efficacité accrue. Reportez-vous aux illustrations suivantes.

Illustration 2 : Les analystes de l'équipe Threat Hunter effectuent un examen approfondi et appliquent leurs informations aux alertes qui présentent une activité suspecte. Leurs commentaires sont placés directement dans la console EDR, de sorte que les équipes SOC ont une vision complète des IOC, ainsi que des personnes et ordinateurs touchés par la menace au sein de l'entreprise.

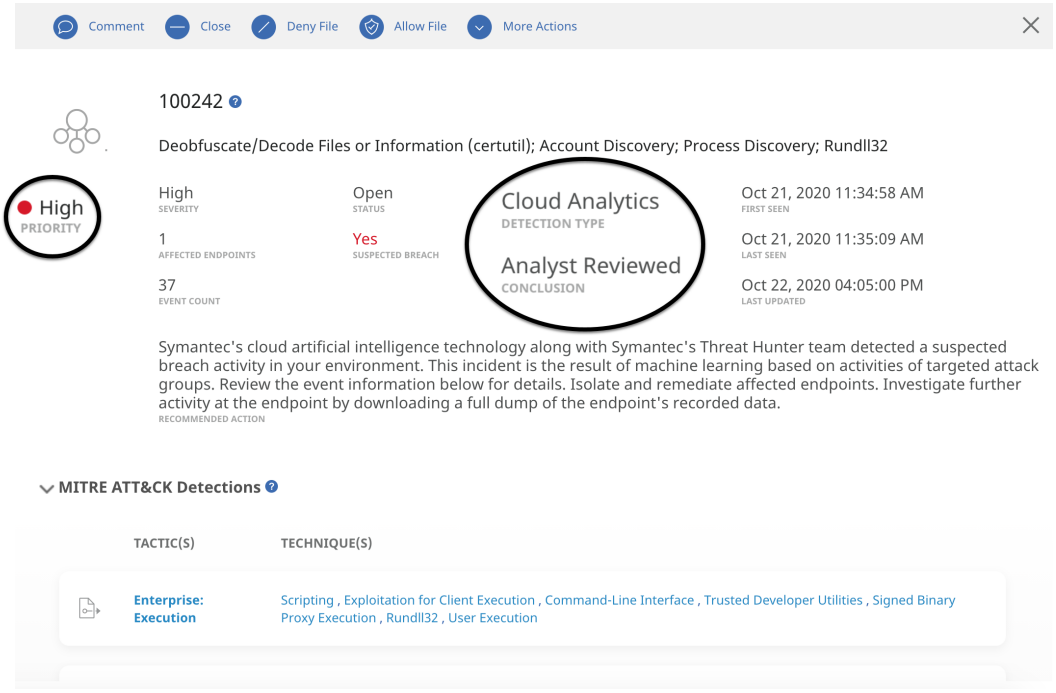
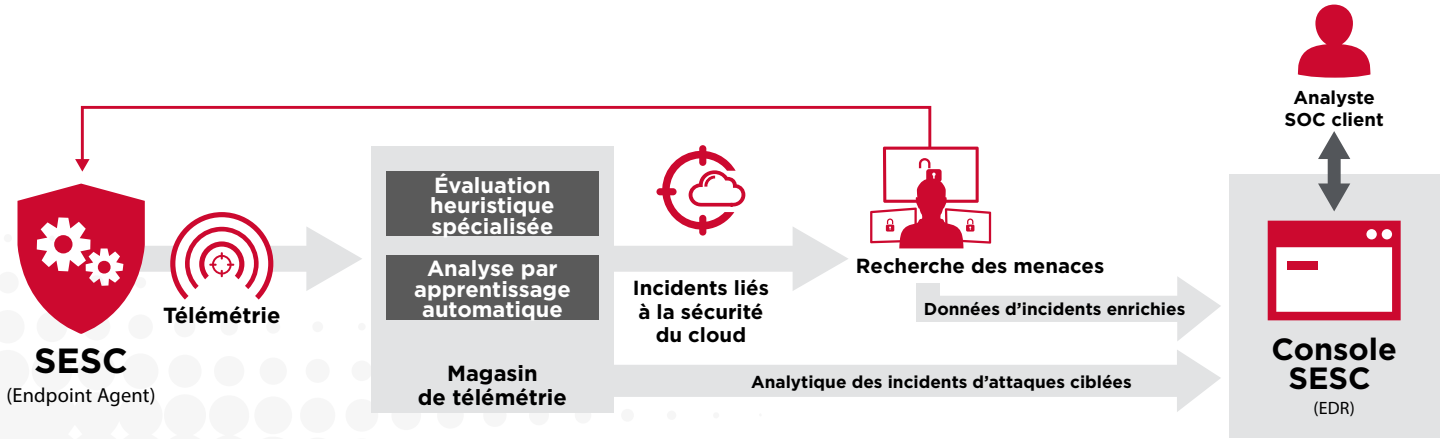


Illustration 3 : Threat Hunter extrait les données de télémétrie de l'agent SESC et les injecte dans le moteur de Machine Learning où les incidents sont identifiés et mis à la disposition des analystes en vue d'un examen plus approfondi. Les analystes appliquent leurs connaissances et outils aux incidents signalés. Ils peuvent également générer d'autres informations pour aider le client à identifier et circonscrire une attaque qui cible son entreprise. À mesure que les incidents identifiés par les analystes sont définis et confirmés, ils sont réinjectés dans les moteurs de Machine Learning de Threat Hunter afin que les incidents ultérieurs de même nature soient immédiatement reconnus.



« Collaborer avec les analystes de l'équipe Threat Hunter de Symantec, c'est l'assurance, pour nos clients, de côtoyer les meilleurs talents en matière de sécurité dans le secteur. »

Threat Hunter met un terme aux méfaits de Cicada

Cicada (connu également sous le nom d'APT10) est un groupe APT dont l'intérêt pour les fournisseurs de services gérés (MSP) et les fournisseurs de services de sécurité gérés (MSSP) est bien connu et largement documenté. En règle générale, lorsqu'un MSP est victime d'une violation de données, cela entraîne des répercussions sur plusieurs entreprises du Fortune X. En avril 2020, les analystes de Symantec ont observé l'activité des menaces en lien avec le groupe Cicada. La cible des menaces était l'un des plus grands MSP et MSSP au monde. Plus récemment, Cicada a ciblé des conglomérats japonais. Une fois encore, cette activité a été découverte par l'équipe Threat Hunter de Symantec.

Activité PowerShell suspecte

Une analyse des attaques ciblées a été déclenchée sur une activité PowerShell suspecte au sein d'une entreprise. Le PowerShell s'est connecté à un serveur distant pour télécharger du contenu et a enregistré des fichiers malveillants supplémentaires sur l'ordinateur. Chaque fichier téléchargé était unique ; le PowerShell était lui aussi, dans chaque cas, en partie unique.

Le pirate n'a utilisé chaque serveur distant que pour un ou deux ordinateurs ciblés, rendant ainsi inutiles les indicateurs de compromission des objets réseau du point de vue de la protection globale.

L'équipe Threat Hunter de Symantec a utilisé la partie PowerShell commune afin de dénicher d'autres activités à travers le globe. Résultat des recherches : une douzaine de serveurs distants diffusaient du contenu vers différentes cibles. Une fois introduit dans la boîte de messagerie électronique de la victime, le pirate informatique a exécuté un certain nombre de scripts liés à la découverte afin de trouver des machines vulnérables, de cartographier le réseau, de vérifier les privilèges et de sonder le contrôleur de domaine. Tous ces outils utilisaient des applications natives installées sur les ordinateurs ciblés. Les cybercriminels ont déployé des efforts considérables pour essayer d'esquiver l'application de sécurité de Symantec en effaçant les journaux système associés aux événements et à PowerShell.

Partage d'informations sur les attaques pour isoler les machines

L'équipe Threat Hunter de Symantec a permis d'éviter une violation de données massive en informant le client que des activités suspectes avaient été repérées sur son réseau. En partageant les détails de l'attaque, l'équipe Threat Hunter a permis au client d'isoler immédiatement les machines affectées, d'utiliser des indicateurs de compromission uniques spécifiques à l'entreprise pour identifier les ordinateurs du réseau qui n'utilisaient pas Symantec Endpoint Protection et d'enquêter sur l'activité malveillante. Grâce à cette interaction proactive avec le client, l'équipe a permis de découvrir l'attaque et de la bloquer avant que d'autres partenaires commerciaux du client ne soient touchés.

« Grâce à leur immense expérience, les chasseurs de menaces de Symantec offrent une vue globale de l'évolution des menaces, tactiques et techniques en dehors de l'environnement SOC. »

Résumé

L'attaque la plus dangereuse et la plus destructrice est celle que vous ne voyez pas venir. À mesure que les attaques gagnent en sophistication et que leur nombre augmente, les entreprises doivent réduire la quantité d'incidents que les analystes doivent examiner et s'assurer que les intervenants se concentrent sur les incidents prioritaires. Pour y parvenir, les équipes de sécurité ont besoin d'aide afin de détecter les attaques réelles. Elles ont besoin de contexte, c'est-à-dire de tout ce qui a trait à l'attaque et à l'assaillant. Protéger l'entreprise exige un rythme de travail effréné. C'est pourquoi les membres de l'équipe doivent pouvoir compter sur des collaborateurs au cas où un élément critique passerait entre les mailles du filet.

Symantec Threat Hunter, une fonction essentielle de SESC, répond à ces besoins. Threat Hunter est un concentré du savoir-faire de Symantec : détections précises sur la base d'une analytique des attaques ciblées, données de télémétrie locales et mondiales, et analyse des attaques réalisée par des chercheurs de renommée mondial

Grâce à Threat Hunter, nous pouvons vous proposer une analyse détaillée de l'assaillant, des techniques et des ordinateurs touchés, ainsi que des conseils de remédiation. Nous offrons à l'équipe SOC la possibilité de mettre rapidement un terme aux incidents qui touchent les terminaux et d'atténuer l'impact des attaques.

Pour plus d'informations, visitez notre site web à l'adresse suivante : www.broadcom.com

SED-Threat-Hunter-WP102_FR 20 novembre 2023