SOPHOS

QUATRE CONSEILS CLÉS D'EXPERTS EN RÉPONSE AUX INCIDENTS

Répondre à un cyber-incident critique peut être une période incroyablement stressante et intense. Bien que rien ne puisse alléger complètement la pression due à la gestion d'une attaque, nos conseils clés d'experts en réponse aux incidents aideront votre équipe à défendre votre organisation.

Ce livre blanc présente les principales leçons à tirer de la réponse aux incidents de cybersécurité. Elles sont le fruit de l'expérience de terrain acquise par les équipes Sophos Managed Threat Response et Sophos Rapid Response, qui ont collectivement répondu à des milliers d'incidents de cybersécurité.

Conseil nº 1 : Réagissez aussi rapidement que possible

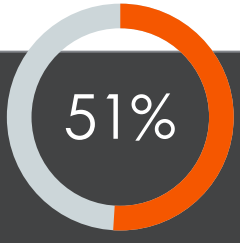
Lorsqu'une organisation est attaquée, chaque seconde compte.

Il y a plusieurs raisons pour lesquelles les équipes peuvent prendre trop de temps à réagir. Le plus souvent, elles ne se rendent pas compte de la gravité et donc de l'urgence de la situation dans laquelle elles se trouvent.

Les attaques ont tendance à frapper aux moments les plus inopportuns : les jours fériés, les week-ends ou au milieu de la nuit. Comme la plupart des équipes de réponse aux incidents manquent cruellement de personnel, certaines tâches sont repoussées au lendemain. Mais malheureusement, le lendemain, il sera peut-être trop tard pour réduire l'impact de l'attaque.

Les équipes débordées sont également susceptibles de ne pas réagir rapidement aux indicateurs d'attaque, car elles sont usées par la surproduction d'alertes. Les signaux se perdent dans le bruit de fond ambiant. Même lorsqu'un dossier de support est initialement ouvert, il peut ne pas être correctement priorisé en raison d'un manque de visibilité et de contexte. Cela est coûteux en temps, et lorsqu'il s'agit de répondre à un incident de cybersécurité le temps ne joue pas en faveur de la victime.

Même dans les situations où l'équipe de sécurité est consciente qu'elle est attaquée et que quelque chose doit être fait immédiatement, elle peut ne pas avoir l'expérience nécessaire pour savoir quoi faire, ce qui la rend également lente à réagir. La meilleure façon de lutter contre ce phénomène est de se préparer en amont à ce type d'incidents.



Plus de la moitié des entreprises ont été touchées par un ransomware l'an dernier, et les attaquants sont parvenus à chiffrer les fichiers dans 73 % des cas.[1]

Conseil nº 2 : Ne criez pas victoire trop tôt

Lorsqu'il s'agit de répondre à un incident, il ne suffit pas de traiter uniquement les symptômes. Il est important de traiter également la maladie.

Lorsqu'une menace est détectée, la première chose à faire est d'établir la priorité des actions à mener. Il peut s'agir de nettoyer un exécutable de ransomware, un trojan bancaire ou encore de bloquer l'exfiltration de données. Toutefois, il arrive souvent que les équipes bloquent l'attaque initiale sans se rendre compte qu'elles n'ont pas vraiment résolu la cause profonde.

Le fait de réussir à supprimer un logiciel malveillant et d'archiver une alerte ne signifie pas que l'attaquant a été éjecté de l'environnement. Il est également possible que ce qui a été détecté n'ait été qu'un test effectué par ce dernier pour évaluer les défenses de la victime. S'il a encore accès à l'environnement, il frappera probablement à nouveau, mais de manière plus forte cette fois.

Les équipes de réponse aux incidents doivent s'assurer qu'elles remédient bien à la cause profonde de l'incident. L'attaquant a-t-il encore un point d'ancrage dans l'environnement ? Prévoit-il de lancer une seconde vague ? Les experts en réponse aux incidents ont remédié à des milliers d'attaques et savent où et quand approfondir leur investigation. Ils analysent tout ce que les attaquants font, ont fait ou prévoient de faire sur le réseau, et les neutralisent.

Par exemple, les experts en réponse aux incidents de Sophos ont réussi à déjouer une attaque qui a duré neuf jours et a vu les attaquants tenter à trois reprises de frapper une organisation avec un ransomware.

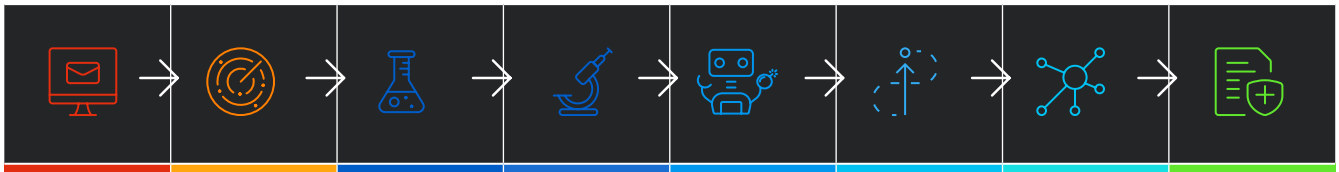
Lors de la première vague de l'attaque (qui a finalement été bloquée par la solution Endpoint de l'organisation), les attaquants ont ciblé 700 ordinateurs avec le logiciel Maze et ont demandé une rançon de 15 millions de dollars. Réalisant qu'ils étaient attaqués, l'équipe de sécurité de la victime a fait appel aux compétences avancées de l'équipe Sophos Managed Threat Response (MTR).

Les experts Sophos ont rapidement identifié le compte administrateur compromis, identifié et supprimé plusieurs fichiers malveillants, et bloqué les commandes de l'attaquant et les communications C2 (Command and Control). L'équipe Sophos MTR a ensuite pu défendre l'organisation contre deux nouvelles vagues d'attaques successives. Si les attaquants étaient parvenus à leurs fins et que la victime avait payé la rançon, cela aurait pu être l'un des paiements les plus chers à ce jour.

Dans un autre exemple, l'équipe Sophos MTR a répondu à une potentielle attaque de ransomware mais n'a pas identifié d'indices concordants. À ce stade, certaines équipes auraient pu clore le dossier et passer à autre chose. Cependant, l'équipe Sophos MTR a continué son investigation et découvert un trojan bancaire historique. Heureusement pour ce client, la menace n'était plus active, mais cela montre l'importance de regarder au-delà des symptômes initiaux afin de déterminer la cause profonde, car cela pourrait être un indicateur d'une attaque plus large.

ÉTUDE DE CAS SOPHOS MTR :

La chasse au ransomware qui a mis au jour un trojan bancaire historique



DÉBUT	15 MINUTES	38 MINUTES	1 HEURE 11 MINUTES	1 HEURE 32 MINUTES	1 HEURE 45 MINUTES	1 HEURE 52 MINUTES	2 HEURES 6 MINUTES
Un client envoie un email pour signaler qu'un fournisseur a été touché par un ransomware. L'équipe Sophos MTR commence immédiatement son investigation pour déterminer si ce client a été touché par l'attaque.	L'équipe MTR ne trouve aucun indice de ransomware, mais détecte le comportement d'un script .js obfusqué que Sophos avait déjà observé et bloqué à l'exécution.	L'équipe MTR envoie des échantillons de fichiers aux laboratoires SophosLabs pour analyse et pour obtenir des indicateurs de compromission (IOC) afin de poursuivre la traque.	Les SophosLabs fournissent des informations complémentaires et une liste d'IOC à l'équipe MTR. Une nouvelle détection est créée pour le script .js afin de protéger tous les clients.	À l'aide des IOC, l'équipe MTR localise un processus qui a déjà appelé un C2. L'équipe est convaincue que cette menace est une variante de Qbot.	Les SophosLabs fournissent d'autres IOC de chemins de fichiers et des informations sur une tâche planifiée avec laquelle le script a interagi. L'équipe MTR continue son investigation.	L'équipe MTR utilise les IOC pour localiser les exécutions historiques, ainsi que le mécanisme de mise à jour et de persistance de la menace.	Dossier classé. L'équipe MTR a supprimé tous les artefacts restants de l'hôte et a fourni au client une synthèse de l'investigation.

Non découvert · Découvert · Triage/Analyse · Confinement/Neutralisation

Conseil nº 3 : Il est crucial d'avoir une visibilité totale

Rien n'est plus difficile pour une organisation que de se défendre à l'aveuglette contre une attaque. Il est important d'avoir accès à des données de qualité, permettant d'identifier avec précision les indicateurs potentiels d'une attaque et d'en déterminer la cause profonde.

Les équipes efficaces sont capables d'extraire les bonnes données pour percevoir les signaux, de séparer ces derniers du bruit de fond et de savoir lesquels doivent être priorisés.

Capter les signaux

Avoir une visibilité limitée sur un environnement est le meilleur moyen de passer à côté d'une attaque. Au fil des ans, de nombreux outils de Big Data ont été mis sur le marché pour tenter de résoudre ce problème spécifique. Certains s'appuient sur des données centrées sur les événements, comme les journaux d'événements, d'autres utilisent des données centrées sur les menaces, et d'autres encore s'appuient sur une approche hybride. Dans tous les cas, l'objectif est le même : collecter suffisamment de données pour générer des résultats utiles pour l'investigation et la réponse aux attaques qui n'auraient autrement pas été identifiées.

La collecte de données de qualité à partir d'une grande variété de sources garantit une visibilité complète sur les outils, tactiques et procédures (TTP) des attaquants. Sans quoi, il est probable que seule une partie de l'attaque serait détectée.

Réduire le bruit de fond

Craignant de ne pas disposer des données nécessaires pour avoir une vue d'ensemble sur une attaque, certaines organisations (et les outils de sécurité sur lesquels elles comptent) collectent tout. Cependant, cela noie l'information dans un océan de données. Non seulement cela augmente le coût de la collecte et du stockage des données, mais cela crée aussi beaucoup de bruit de fond, entraînant une surproduction d'alertes et faisant perdre un temps précieux aux équipes qui doivent vérifier les faux positifs.

Utiliser le contexte

Les experts en réponse aux incidents ont une maxime qui dit : « Si le contenu est roi, le contexte est reine. ». En effet, ces deux éléments sont nécessaires pour mettre en œuvre un programme efficace de réponse aux incidents. Utiliser des métadonnées significatives associées aux signaux permet aux analystes de déterminer si ces derniers sont malveillants ou bénins.

L'un des éléments clés d'une réponse efficace aux menaces est de prioriser les signaux les plus importants. La meilleure façon de repérer les alertes critiques est de combiner le contexte fourni par les outils de sécurité (c'est-à-dire les solutions EDR [Endpoint Detection and Response]), l'intelligence artificielle, les données d'intelligence sur les menaces et la base de connaissances de l'opérateur humain.

Le contexte permet de déterminer l'origine d'un signal, le stade actuel de l'attaque, les événements connexes et l'impact potentiel sur l'entreprise.

Conseil nº 4 : Il n'y a pas de mal à demander de l'aide

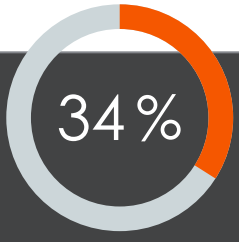
Aucune organisation ne tient à faire face à une tentative de violation. Cependant, rien ne remplace l'expérience lorsqu'il s'agit de répondre à un incident. Cela signifie que les équipes informatiques et de sécurité chargées de répondre aux incidents critiques se retrouvent dans des situations où elles n'ont tout simplement pas les compétences nécessaires pour y faire face ; des situations qui ont souvent un impact considérable sur l'entreprise.

Le manque de personnel qualifié capable d'analyser et de répondre aux incidents est l'un des plus grands problèmes auquel est confronté le secteur de la cybersécurité aujourd'hui. Ce problème est tellement répandu que selon ESG Research[2], « pour 34 % des entreprises, le plus grand défi est le manque de personnel qualifié pour analyser les incidents de cybersécurité impliquant un système d'extrémité afin de déterminer la cause profonde et la chaîne d'attaque ».

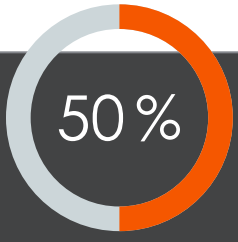
Une solution alternative est née de cette situation : les services de sécurité managés. Plus précisément, les services managés de détection et de réponse (MDR). Les services MDR correspondent à des opérations de sécurité externalisées, assurées par une équipe de spécialistes, qui agissent comme une extension de l'équipe de sécurité des clients. Ces services combinent des opérations réalisées par des experts (investigations, traque des menaces, surveillance en temps réel et réponse aux incidents) avec un ensemble de technologies pour recueillir et analyser les données d'intelligence. Selon le Gartner, « d'ici 2025, 50 % des organisations utiliseront des services MDR »[3], ce qui démontre que celles-ci se rendent compte qu'elles auront besoin d'aide pour mener à bien un programme complet d'opérations de sécurité et de réponse aux incidents.

Pour les organisations qui n'utilisent pas de services MDR et qui font face à une attaque active, les services d'experts en réponse aux incidents sont une excellente option. Ces experts sont appelés lorsque l'équipe de sécurité de l'organisation est débordée et a besoin d'une aide extérieure pour traiter l'attaque et s'assurer que l'attaquant a été neutralisé.

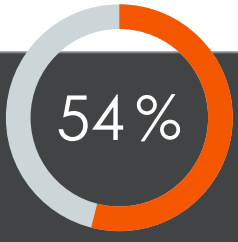
Même les organisations qui disposent d'une équipe d'analystes de sécurité compétents peuvent tirer profit d'une collaboration avec un service de réponse aux incidents, notamment pour couvrir toutes les plages horaires (c'est-à-dire les nuits, les week-ends, les jours fériés) et pour disposer de toutes les compétences spécialisées nécessaires pour répondre aux incidents.



Selon le cabinet d'analystes ESG, pour 34 % des entreprises, le plus grand défi est le manque de personnel qualifié pour analyser les incidents de cybersécurité impliquant un système d'extrémité afin de déterminer la cause profonde et la chaîne d'attaque.[2]



D'ici 2025, 50 % des entreprises auront recours à des services MDR (contre moins de 5 % en 2019).[3]



Dans une enquête menée en 2019 auprès de 3 100 responsables IT et professionnels de la cybersécurité, 54 % des répondants ont déclaré « ne pas être en mesure d'exploiter pleinement leur solution » à cause d'un manque de compétences.[4]

Comment Sophos peut vous aider

Service Sophos Managed Threat Response (MTR)

Vous vous inquiétez de la capacité de votre organisation à répondre à un incident potentiellement grave ? Si c'est le cas, le service Sophos Managed Threat Response (MTR) est une option qui mérite d'être envisagée.

Sophos MTR est une offre de services de recherche, de détection et de réponse aux menaces, entièrement managée par une équipe d'experts 24 h/24 et 7 j/7. L'équipe Sophos MTR ne se contente pas de vous notifier lorsqu'une attaque ou un comportement suspect sont identifiés, mais intervient à votre place pour neutraliser les menaces les plus sophistiquées et les plus complexes à l'aide d'actions ciblées. Si un incident se produit, l'équipe MTR lancera des actions à distance pour intercepter, contenir et neutraliser la menace. L'équipe d'experts en opérations de sécurité fournit également des conseils pratiques pour traiter les causes profondes des incidents récurrents.

Consultez www.sophos.fr/mtr pour en savoir plus.

Service Sophos Rapid Response

Si votre organisation est attaquée et a besoin d'une assistance immédiate pour répondre à un incident, Sophos peut vous aider.

Piloté par une équipe d'experts en réponse aux incidents, le service Sophos Rapid Response identifie et neutralise de manière ultra-rapide les menaces actives ciblant les organisations. La prise en charge (onboarding) s'effectue en quelques heures et la majorité des clients font l'objet d'une priorisation (triage) sous 48 h. Le service est disponible à la fois pour les clients Sophos actuels, mais aussi pour les non-clients Sophos.

L'équipe Sophos Rapid Response est composée d'experts en réponse aux incidents qui prennent rapidement des mesures à distance pour prioriser, contenir et neutraliser les menaces actives. Les attaquants sont expulsés de votre parc informatique pour empêcher d'autres dommages.

Consultez www.sophos.fr/rapidresponse pour en savoir plus.

Sophos Intercept X Advanced with EDR

Les organisations qui souhaitent augmenter en interne leur capacité de détection, d'investigation et de réponse aux incidents devraient s'intéresser aux capacités de Sophos EDR (Endpoint Detection and Response).

Sophos Intercept X Advanced with EDR permet à votre équipe de traquer les menaces et de maintenir l'hygiène de vos opérations informatiques sur l'ensemble de votre parc informatique. Sophos EDR permet à votre équipe de poser des questions détaillées pour identifier les menaces avancées, les attaquants actifs et les failles informatiques potentielles, puis de prendre les mesures appropriées pour les bloquer.

Consultez www.sophos.fr/edr pour en savoir plus et démarrer un essai gratuit.

[1] Enquête réalisée en 2020 auprès de 5 000 DSI https://secure2.sophos.com/fr-fr/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx

[2] https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1

[3] Gartner, Market Guide for Managed Detection and Response Services, 26 août 2020, Analystes : Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

[4] Enquête réalisée en 2019 auprès de 3 100 DSI https://secure2.sophos.com/fr-fr/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

20-10-30 WPFR (PS)

SOPHOS