FORTINET

Les 5 fonctionnalités clés d'une plateforme de détection et réponse aux cybermenaces

Table des matières

Synthèse

Les compétences pointues des cybercriminels actuels et leurs attaques sophistiquées sont un vrai défi pour les équipes opérationnelles de sécurité. Une cyberdéfense robuste implique de surveiller de multiples vecteurs d'attaque et une pléthore de signaux d'activité malveillante, une tâche assurément complexe et chronophage. Les professionnels de la sécurité les plus expérimentés le savent : c'est en déployant les technologies pertinentes que votre équipe bénéficiera d'une visibilité globale sur leur infrastructure de sécurité et des moyens de juguler un incident avant tout dommage. Lorsque vous évaluez des solutions de détection et de réponse, certaines questions essentielles s'imposent avant d'investir.

Introduction

Lorsqu'elles investissent dans la cybersécurité, la plupart des entreprises se sont historiquement concentrées sur la prévention des menaces. Mais comme le souligne une note d'étude de Gartner, « face à une détection des menaces qui se veut complexe, il n'est plus possible de se contenter d'investir dans un seul produit de prévention des menaces. Il s'agit de privilégier un panel de fonctionnalités de détection qui recueille suffisamment d'indicateurs via diverses méthodes, y compris des API, puis analyse ces indicateurs pour repérer une éventuelle attaque. »[1]

Ceci étant dit, les dirigeants d'entreprise sont conscients de la complexité de leur infrastructure de sécurité et du défi que représente la gestion des alertes. Cependant, et c'est une bonne nouvelle, 75 % des entreprises cherchent à consolider le nombre de leurs fournisseurs de solutions de cybersécurité, en privilégiant une plateforme à un ensemble de produits distincts et autonomes.[2]

Sur le terrain, toutes les plateformes n'offrent pas le périmètre de couverture nécessaire. La prise en charge de la surface d'attaque et des différentes étapes d'une campagne d'attaques, les performances des technologies de détection et le degré d'intégration varient considérablement d'une solution à l'autre. Enfin, si le sujet de la technologie est celui qui reçoit le plus d'attention, il n'empêche que les personnes et les processus jouent un rôle essentiel pour assurer une défense efficace. Comme le reconnaît à juste titre Gartner, « le panel technologique qui vous convient le mieux est celui qui répond le plus efficacement et à moindre coût à vos objectifs de monitoring. »[3]

Cinq questions à se poser avant d'investir dans la détection et la réponse aux menaces

Supposons que vous envisagez d'opter pour une plate-forme de détection et de réponse des menaces ou que vous devez personnaliser votre approche de gestion des risques. Dans ces cas, il convient de se poser cinq questions essentielles avant d'investir.

1. Que pouvez-vous inspecter ?

Les assaillants tentent de s'immiscer dans votre entreprise via différents vecteurs (email, téléchargement sur Internet, applications et ressources accessibles depuis l'extérieur, services d'entreprise, etc.) pour s'en prendre à des cibles en interne (dispositifs d'utilisateurs finaux, serveurs applicatifs, systèmes IoT et OT, etc.) ou en externe (Software-as-a-Service et infrastructure de cloud public par exemple).

Comme récemment mentionné par Gartner, « la diversité des perspectives offertes par un panel technologique résulte des différents types et du volume de menaces pouvant être détectées, et/ou de la fiabilité des alertes générées. A minima, le panel doit offrir une visibilité sur

les menaces présentant le plus d'intérêt ».[4] Sans inspection, impossible de détecter les menaces, ce qui implique de surveiller tous les vecteurs d'attaque et les infrastructures ciblées.

2. Toutes les étapes d'une attaque sont-elles prises en charge ?

Nombre d'attaques s'exécutent en plusieurs étapes pour contourner les fonctions préventives de sécurité, rester furtives sur de longues périodes, maximiser leur impact et optimiser leur retour sur investissement. Le framework MITRE ATT&CK et la chaîne de frappe (kill chain) telle que définie par Lockheed Martin témoignent des étapes classiques et des tactiques régulièrement utilisées lors des attaques, de la phase de préparation, à l'exécution de l'attaque et aux phases post-infection et post-intrusion. Heureusement, plus l'assaillant exécute des étapes avant d'atteindre son objectif final, plus l'entreprise ciblée peut détecter et perturber l'attaque avant qu'elle ne réussisse.

Selon Gartner : « En général, les fonctionnalités de détection doivent être actives au niveau de chaque étape d'une attaque. Elles doivent déclencher des alertes fiables, nécessaires à vos tâches de monitoring ».[5] Pour ce faire, une plateforme de sécurité opérationnelle doit prendre en compte tous les vecteurs d'attaque et de propagation, ainsi que chacune des étapes de la chaîne de frappe (reconnaissance, armement, livraison, exploitation, installation, communications Command & Control, et actions post-infection).

3. Quelles sont les technologies de détection ?

Bien entendu, ce n'est pas parce que vous inspectez l'activité au niveau des vecteurs d'attaque et de la chaîne de frappe cyber que vous identifierez automatiquement les attaques. En effet, ces dernières sont souvent élaborées pour ressembler à des services ou des actions légitimes, si ce n'est pour les utiliser. Selon Gartner, « certaines méthodes sont simples à identifier, certaines exigent une connaissance approfondie des menaces, et d'autres peuvent nécessiter un traitement analytique complexe de données de sécurité. L'efficacité des méthodes dépend du type de menace. »[6]

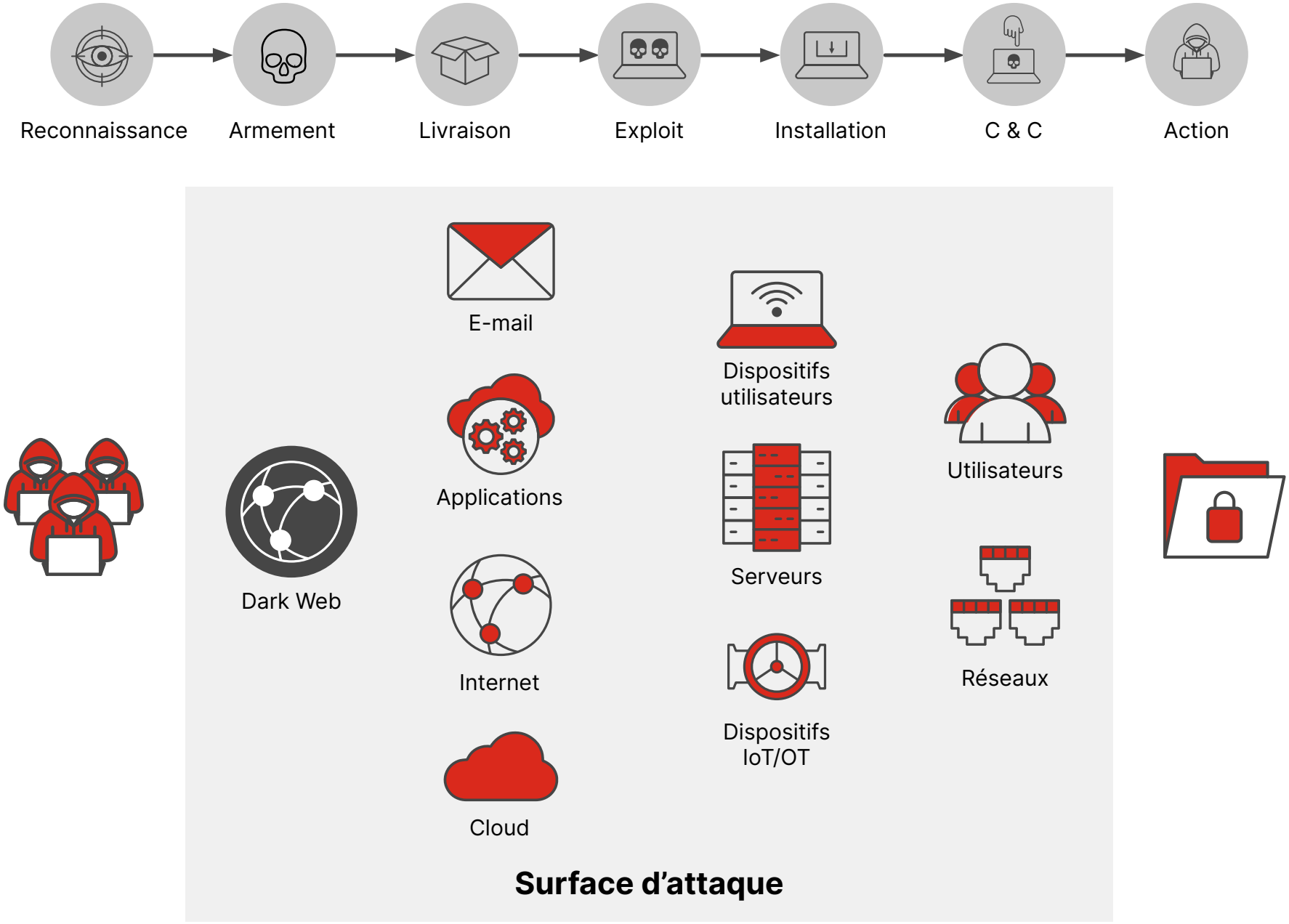

Schéma 1 : gestion de la surface d'attaque et de la chaîne de frappe

Une veille sur les menaces et les indicateurs de compromission sont certes précis, mais restent peu prédictifs. Les règles et les analyses heuristiques sont plus prédictives mais elles génèrent souvent des faux positifs. Les modèles statiques de machine ou deep learning sont beaucoup plus prédictifs mais ils offrent généralement un système de probabilités auquel il n'est pas simple de faire confiance initialement, ou dont la maintenance est complexe dans le temps. L'analyse comportementale n'offre des données de prédiction fiable que si les processus sous-jacents identifient avec précision les tactiques, techniques ou procédures connues. L'identification d'une activité anormale, que celle-ci soit légitime ou prohibée, est chronophage pour les équipes de sécurité. Il s'agit donc d'adapter le mix de technologies de détection à votre entreprise et à votre équipe.

4. Quelles sont les modalités de la réponse aux menaces ?

La détection est une étape initiale : la validation de l'incident et son confinement s'imposent pour maîtriser les risques. D'autre part, une investigation complète et un processus de remédiation sont nécessaires pour revenir à un opérationnel sûr.

Traditionnellement, cette investigation est menée manuellement par des professionnels expérimentés de la sécurité. Cependant, selon Gartner, « des procédures opérationnelles

standards de réponse s'imposent pour définir les objectifs, les processus et les tâches. Cependant, elles ne permettent pas de prévoir, sur la base du type spécifique d'attaque qui s'est produit, ce qui est nécessaire pour prendre en charge chaque élément impliqué dans cette attaque. »[7]

Les entreprises doivent décider si elles vont tirer parti des connaissances de leur équipe de sécurité ou si elles préfèrent fédérer ces connaissances au sein de processus documentés qui permettront à une plateforme d'orchestrer et d'automatiser la sécurité. Une stratégie opérationnelle s'appuie généralement sur ces deux approches et les entreprises doivent déterminer le bon équilibre.

5. Votre équipe peut-elle gérer la solution ?

Bien entendu, même le système le mieux outillé, orchestré et automatisé ne peut fonctionner seul. Comme le précise Gartner : « Le dernier défi, souvent difficile, est celui de l'opérationnel… La majeure partie du travail à réaliser n'est pas liée aux dysfonctionnements et aux opérations, mais prend plutôt la forme d'une réflexion critique et d'investigations menées par des experts. »[8]

Votre plateforme de détection et de réponse choisie peut être gérée par votre équipe, ou vous pouvez faire appel à des experts externes. Cette externalisation, ponctuelle ou permanente, peut porter sur l'ensemble des activités ou ne concerner que certaines tâches. Dans tous les cas, l'externalisation, qui consiste à faire appel à des compétences externes, n'exonère pas l'entreprise des risques cyber. Si cette option est retenue, assurez-vous de sélectionner une plateforme proposée par un partenaire fiable disposant de l'expertise nécessaire.

Synthèse

Les compétences sophistiquées des assaillants et la complexité de leurs attaques constituent un vrai défi. Mais c'est également l'opportunité de vous assurer que vous disposez d'un système de détection efficace couvrant l'ensemble de la surface d'attaque et de la chaîne de frappe d'une attaque. Vous devez opter pour une technologie fiable qui assure une réponse pertinente aux menaces, pour ainsi garder la main sur vos risques cyber.

[1] The Journey to SOC in Three Steps : Step 2 Building the Detection Stack and Establishing Security Operations, Gartner, 19 décembre 2022.

[2] Gartner Survey Shows 75% of Organizations are Pursuing Security Vendor Consolidation in 2022, Gartner, 13 septembre 2022.

[3] The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations, Gartner, 19 décembre 2022.

[4] Idem.

[5] Idem.

[6] Idem.

[7] Idem.

[8] Idem.

FORTINET

www.fortinet.com/fr

mars 22, 2024 1:31 PM

2504903-0-0-EN