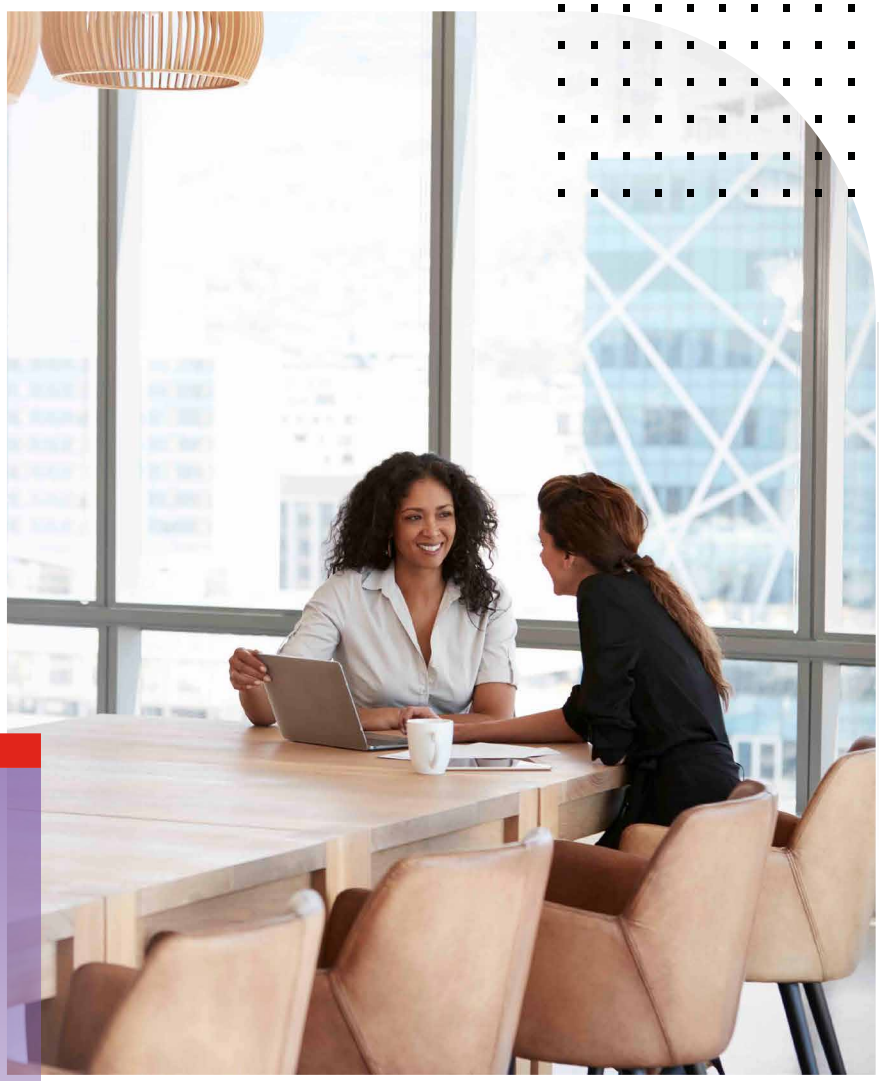
LIVRE BLANC

Évaluez la sécurité de vos endpoints

Évaluations MITRE Engenuity ATT&CK : mieux cerner vos capacités



Synthèse

Choisir un outil de sécurité pertinent relève souvent de la gageure. D'où l'intérêt de disposer d'informations indépendantes et objectives. Les entreprises sont invitées à tirer parti des résultats de l'évaluation MITRE Engenuity ATT&CK pour statuer sur l'efficacité des solutions de sécurité endpoint. Elles sont également en mesure d'évaluer leur posture de sécurité actuelle, à l'aide des outils MITRE, et ainsi identifier leur capacités et carences en matière de détection. Elles peuvent, par la suite, comparer leurs résultats à la liste MITRE des tactiques et techniques qu'utilisent les cybercriminels pour mener leurs attaques.

La sécurité des endpoints revient à en maîtriser les risques. Ainsi, avant d'évaluer les solutions, les professionnels de la sécurité doivent s'assurer de disposer d'une base solide. Les bonnes pratiques de sécurité permettent ainsi de maîtriser l'exposition aux risques. De leur côté, les professionnels de la sécurité doivent disposer d'une stratégie pour renforcer leur posture de sécurité et leur visibilité sur celle-ci.
Une fois ces fondamentaux en place, il devient pertinent de consulter des tests indépendants pour sélectionner la solution la plus adaptée à ses besoins.

L'EDR (endpoint detection and response) a été la réponse la plus souvent citée par les entreprises interrogées sur leurs investissements prioritaires en sécurité endpoint, sur les 12-18 mois à venir.[1]

Un comparatif objectif des produits

L'univers des menaces, en constante évolution, donne lieu à des versions successives d'attaques existantes, ainsi qu'à de toute nouvelles cybermenaces. Il est essentiel que la posture de sécurité d'une entreprise et ses fonctions de sécurité en place soient robuste. Cependant, les produits de cybersécurité restent difficiles à évaluer, compte tenu des différentes approches et termes utilisés pour décrire leurs fonctionnalités. Les tests menés par des tiers pour évaluer les produits permettent de les comparer, fonction par fonction, pour prendre des décisions plus pertinentes et identifier la solution adaptée à leur situation actuelle et au niveau de sécurité cible. Cependant, il est parfois complexe de déterminer la réelle valeur de ces tests sur l'infrastructure de sécurité, lorsque ces tests font office de « boîtes noires » qui se contentent de donner des résultats (menace neutralisée ou pas, détectée ou pas) plutôt que d'expliciter leur mode opératoire.

MITRE ATT&CK Evaluations

Depuis 2019, les évaluations MITRE testent de manière objective et détaillée les capacités des solutions de sécurité endpoint, en émulant les techniques et tactiques qu'utilisent réellement les assaillants. Les méthodes d'émulation capitalisent sur des informations de veille sur les cybermenaces. Elles sont mises en correspondance avec un ensemble de techniques et tactiques ATT&CK et utilisées pour répliquer des comportements qui évaluent objectivement les performances des produits. Les résultats révèlent la capacité technique d'une solution à détecter une campagne d'attaques spécifique. Ils démontrent également les techniques et tactiques couramment utilisées par nombre de cybermenaces actuelles.

Les évaluations MITRE Engenuity ATT&CK sont pertinentes car basées sur le framework MITRE ATT&CK, une base de connaissances des techniques utilisées par les assaillants. Ce framework offre une ventilation et une classification des actions offensives des assaillants contre des plateformes précises comme Windows. Contrairement à d'autres travaux menés sur ce sujet, l'accent n'est pas mis sur les outils et malware utilisés par les adversaires, mais sur leur interaction avec les systèmes lors de leurs opérations.

De manière générale, le framework ATT&CK organise les techniques en des ensembles de tactiques. Chaque technique donne lieu à des informations pertinentes qui aident les entreprises à comprendre les évènements et implications de cette technique, lorsqu'utilisée. Les liens entre les tactiques et les techniques sont présentés dans la Matrice ATT&CK, qui couvre 11 techniques différentes. La matrice offre un mapping précis de l'activité des cyberattaques potentielles. Chaque domaine, qui compte 10 tactiques ou plus, couvre de l'accès initial jusqu'aux communications Command & Control.

L'opus 2020 des évaluations ATT&CK porte sur l'émulation de Carbanak, un groupuscule ciblant les banques, ainsi que FIN7, un groupe à but lucratif qui a ciblé les secteurs de la grande distribution, de la restauration et de l'hôtellerie aux USA, souvent à l'aide d'un malware ciblant les systèmes de point de vente. Les cas testés sont particulièrement pertinents car ils :

- Utilisent le scripting, l'obfuscation, la dissimulation de malware et le piratage d'utilisateurs en aval des machines.
- Utilisent des techniques opérationnelles uniques basées sur des malware sophistiqués et sur des outils d'administration légitimes, capables d'interagir avec différentes plateformes.

En 2020, MITRE a étendu le périmètre des évaluations en intégrant des résultats de détection et/ou des résultats de protection. Qu'une technique ou tactique ait été détectée sur un périmètre où elle aurait pu être neutralisée, la principale différence est que, une fois la tactique neutralisée, aucune évaluation des activités à une étape ultérieure n'était possible.

Test de détection

En matière de tests de détection, les évaluations portent sur 20 scénarios. Chaque test présente de multiples étapes. Les évaluations utilisent 6 termes pour décrire les performances de chaque produit lors de chaque test et note également les sources de données pour la détection.

- **Not Applicable.** Le constructeur n'a pas déployé de capteur sur le système de test.
- **None.** Aucune donnée identifiée n'indique que le comportement du test a été détecté par le produit.
- **Télémetrie.** Le comportement à été identifié mais traité de manière minimale.
- **General.** Le comportement a été identifié et traité, mais sans information détaillée sur pourquoi (tactique) et comment (technique) l'action a été réalisée.
- **Tactic.** Le comportement a été traité et identifié comme malveillant, avec des informations sur la tactique utilisée et les raisons de son utilisation par la cyberattaque.
- **Technique.** Le comportement a été traité et identifié comme malveillant, avec des informations sur la technique utilisée et son mode opératoire lors de la cyberattaque.

Lorsqu'un test de détection, une tactique ou une technique est identifiée comment « Not applicable », il est important d'en connaître la raison. Il peut s'agir d'une non-compatibilité à un système d'exploitation (ou similaire) lors du déploiement du produit. Il est également possible que le produit n'ait pas été conçu pour identifier les comportements émulés lors du test. Il peut s'agir d'autres raisons pouvant être importantes ou pas pour votre entreprise.

Lorsque les comportements testés sont souvent associés à des opérations potentiellement légitimes, ou malveillantes, la mention « None » n'indique pas forcément un résultat négatif, notamment si le risque de laisser passer ce comportement est également « None ». C'est notamment le cas lorsqu'un cybercriminel n'est pas arrivé à ses fins.

« Telemetry » ou « General » constituent les premiers niveaux de détection d'un comportement identifié et enregistré par un produit. Il y a néanmoins peu de détails sur les raisons de cette identification. Ce niveau est suffisant pour les entreprises qui manquent e temps et d'expertise pour connaître dans le détail comment le cybercriminel tente de mener sa mission. Les détections reconnues en tant que « Tactic » ou « Technique » vont intéresser les professionnels de la sécurité qui souhaitent connaître l'activité cybercriminelle dans le détail.<558></558>

Tests de Protection

Les tests de protection utilisent trois termes.

- **Not applicable.** Idem que pour les tests de détection. Peut également indiquer que le test a été interrompu en amont des techniques à suivre.
- **None.** Aucune preuve que la technique incriminée à été neutralisée grâce au produit.
- **Blocked.** La technique a été neutralisée et l'utilisateur en a été informé.

Même si le nombre de termes est moindre, l'interprétation est plus complexe. En effet, le moment où la technique est neutralisée, une information importante, peut varier selon le test. Les faux-positifs ne sont pas évalués, mais plus la neutralisation s'effectue en amont, plus les faux-positifs sont susceptibles d'être nombreux. En revanche, une neutralisation tardive peut exposer l'entreprise à un niveau élevé de risques, même si l'objectif final n'est pas atteint. Voici de exemples de chaque scénario :

Supposons que le Test 1 entraîne une neutralisation à la première étape 1.a.1. La cyberattaque a été neutralisée à l'étape la plus amont possible. Mais quid si c'est, en réalité, l'accès d'un utilisateur qui est neutralisé ? Dans ce cas, vous aimeriez sans doute savoir la raison pour laquelle l'accès de l'utilisateur à un fichier a été bloqué, non ? S'agit-il d'un indicateur d'un acte malveillant ? Où les règles ont-elle été définies de manière trop strictes ? D'autre part, imaginons, que la neutralisation s'opère à la fin, à l'étape 2.b.5 d'exfiltration de données via un canal Command & Control. Dans ce cas, le produit neutralise le piratage de données, mais a laissé passé l'étape step 2.b.1 (copie de fichier à distance), ce qui indique que l'attaque à eu un impact malveillant.

Dans ce cas particulier, l'étape 1.a.3 aurait dû être le meilleur moment pour neutraliser l'attaque afin de minimiser les faux-positifs, compte tenu des « preuves » recueillies et de l'impact des actions malveillantes. Cette étape intervient lorsqu'un script effectue la première manipulation malveillante de fichier. Mais cette information ne peut être déterminée qu'après avoir bien compris les sous-étapes de chaque étape. Le succès ou l'échec dépendent de la volonté de chaque entreprise de préserver l'activité légitime des utilisateurs en dépit du risque d'impact important d'une cyberattaque.

Rappel important sur les résultats des évaluations

MITRE insiste sur le fait que les évaluations ne constituent pas une analyse concurrentielle. Il n'y a pas de score, de classement ou de « lauréats ». Ces évaluations visent à répertorier les détections et à observer l'approche de chaque constructeur en matière de détection des menaces, selon le référentiel ATT&CK. Ces évaluations apportent ainsi aux entreprises des réponses aux questions suivantes :

- L'outil évalué détecte-t-il les menaces connues ciblant votre entreprise ?
- Comment l'outil restitue-t-il les données à vos analystes ?
- Est-il capable d'arbitrer entre détection/protection stricte et risque potentiel de piratage ?

Fortinet participe aux évaluations MITRE ATT&CK 2020 portant que le scénarios d'attaque Carbanak+FIN7.

Les évaluations vous indiquent quels sont les fournisseurs qui vous proposent la meilleure visibilité sur les techniques des assaillants, ainsi que les constructeurs qui répondent le mieux aux techniques qu'utilisent les menaces. Une évaluation vous indique les perspectives dont vous bénéficierez, ainsi que la fréquence de mise à jour de la solution pour faire face aux techniques des assaillants. Les évaluations vous précisent également si un outil utilise une interface graphique, si elle offre des options clés-en-mains à l'intention d'analystes juniors, ou si elle propose des données bruts à l'intention d'analystes plus expérimentés.

Cependant, ces évaluations ne peuvent répondre aux questions suivantes :

- Quel est l'impact sur les systèmes et les utilisateurs ?
- Quel est le volume d'alertes et les recherches manuelles qui sont nécessaires ?
- Comment l'outil s'intègre-t-il au sein de votre environnement de sécurité ? Vient-il l'enrichir ? Ou s'agit-il d'un doublon ?
- Des actions légitimes sont-elles neutralisées par erreur ?
- Comment l'outil s'intègre-t-il avec les autres outils ?
- Quel est le coût de l'outil ?

Les réponses à ces questions impliquent des travaux de recherche et des tests supplémentaires, avec prise en compte d'une image plus globale de votre entreprise.

Les enseignements de ces évaluations

La plus grande valeur des tests MITRE est qu'ils démontrent la capacité d'un produit à juguler les tactiques et techniques utilisées par des échantillon d'attaque. Avec ces évaluations, vous pouvez déterminer votre exposition à des attaques inconnues, sur la base des tactiques et techniques utilisées. Une alternative à une évaluation du niveau de sécurité par rapport à des modèles et référentiels de veille sur les menaces.

Les DSSI tirent parti des évaluations de MITRE Engenuity ATT&CK pour identifier les carences de sécurité de leur entreprise. Aucune solution ne peut détecter toutes les attaques et techniques existantes, mais il est possible de connaitre les produits identifiant un type précis d'attaque. Les entreprises doivent déployer une approche intégrée qui leur permettrait de :

- Détecter et neutraliser les menaces au plus tôt dans le cycle d'une attaque
- Moduler la confiance dans un évènement plutôt que de leur bloquer en amont
- Comprendre comment une solution jugule une menace. Permet-elle de neutraliser des actions malveillantes spécifiques en temps réel et de les isoler ? Ou la solution se base-t-elle sur le cloisonnement du réseau pour prévenir les mouvements internes des menaces ?
- N'appliquer les capacités strictes des outils (mise à l'arrêt des processus, mise en quarantaine des endpoints) que lorsque vraiment nécessaire
- Simplifier les opérations de sécurité

Perspectives

La sécurité des endpoints est plus que jamais essentielle. Les attaques dynamiques, à l'instar de celles basées sur les ransomware, ne prennent que quelques minutes pour réussir. Leur prise en charge manuelle, comme le proposent les outils EDR de première génération, ne suffit plus. L'objectif d'une infrastructure robuste de cybersécurité, pour les endpoints notamment, est de maîtriser le risque de manière globale. Des règles de sécurité efficaces et un monitoring continu doivent être déployés pour prévenir, identifier et répondre aux attaques, tout en assurant la remédiation post-incident.

La découverte et la prévention des menaces sont des pratiques essentielles de sécurité qui permettent de maîtriser les risques. Cependant, chaque DSSI s'accorde à penser que la prévention ne peut être efficace à 100 %.

Ainsi, au-delà de la prévention, les entreprises doivent détecter efficacement les menaces au plus tôt, traiter et juguler les menaces rapidement pour neutraliser un piratage, et, enfin, assurer les opérations de restauration. In fine, l'objectif est de minimiser les perturbations sur les opérations métiers et de favoriser la résilience des entreprises.

Les évaluations MITRE ATT&CK aident les entreprises à jauger le solutions de sécurité endpoint compte tenu de leur capacité à détecter et, dans une certaine mesure, à prévenir les menaces. Cependant, lorsque les entreprises recherchent un outil de sécurité endpoint, elles doivent aller au-delà des résultats MITRE et :

- Mettre en place des bonnes pratiques de sécurité (découverte, prédiction) pour réduire la surface d'attaque, avec une visibilité et des fonctions proactives de protection jusqu'à application des patchs de sécurité.
- Améliorer la précision pour réduire l'impact des faux-positifs et éviter d'avoir à trier des alertes trop nombreuses
- Se focaliser sur la maîtrise de l'impact, via une prise en charge automatisée et précise des menaces qui améliorent la gestion des risques
- Pérenniser la haute-disponibilité et la stabilité des systèmes, même lors d'une attaque, notamment pour les technologies OT et les systèmes critiques
- Tirer le meilleur parti de la technologie. Aucun outil n'est capable de se déployer, d'opérer et d'assurer sa maintenance de manière autonome

Conclusion

MITRE ATT&CK Evaluations est un framework qui va au-delà d'une simple notation de l'efficacité d'un produit de sécurité, pour, au final, explorer son mode opératoire. Cette approche présente l'avantage de mieux comprendre les fonctionnalités que vous déployez. En l'associant à d'autres évaluations, vous pouvez aller au-delà des échantillons retenus pour réaliser les tests. MITRE ATT&CK Evaluations permet de sélectionner le produit de sécurité endpoint qui maîtrise les risques de cybersécurité dans des domaines essentiels, tout en gérant l'impact sur les collaborateurs, les processus et les systèmes. Ces évaluations déterminent également si une solution est adaptée à votre infrastructure de sécurité en général.

Cependant, aucune solution de sécurité n'est parfaite. Certaines techniques ne peuvent être détectées à l'échelle du endpoint uniquement. Parallèlement, certains comportements peuvent être identifiés par plusieurs solutions. Il est préférable d'avoir des outils dont le périmètre fonctionnel se chevauche, plutôt que de subir des carences en sécurité. D'autre part, un faible niveau d'intégration constitue un vrai défi.

[1] David Gruber, "ESG Master Survey Results: Trends in Endpoint Security," ESG, 5 mars 2020.

FORTINET

www.fortinet.com/fr

août 17, 2021 9:31 AM
wp-FA-assess-your-endoint-security-4202021-A4
968201-0-1-FR