Vidéos explicatives

Articles explicatifs originaux issus de la vidéothèque de Cyber Crucible — rançongiciels, vol de données, usurpation d'identité, sécurité autonome et FortressAI — chacun accompagné de la vidéo correspondante.

- Les entreprises réagissent-elles de manière excessive face au risque lié à l'IA, ou s'agit-il d'un problème de visibilité ?
- Pourquoi les modèles traditionnels de SOC peinent-ils face aux cyberattaques à vitesse machine ?
- À quoi ressemble concrètement une cybersécurité véritablement autonome au quotidien ?
- Les outils d'IA comme ChatGPT peuvent-ils remplacer une équipe humaine de cybersécurité ?
- Les rançongiciels peuvent-ils toujours atteindre les données stockées dans des services cloud comme OneDrive ou Google Drive ?
- Si un rançongiciel s'autodétruit, cela signifie-t-il que l'attaque est terminée ?
- La cybersécurité doit-elle se concentrer sur la résilience ou sur la prévention des attaques dès le départ ?
- Comment Cyber Crucible m'aide-t-il à gérer les fournisseurs de cybersécurité et les résultats ?
- Comment Cyber Crucible m'aide-t-il à maîtriser mes dépenses de cybersécurité et mes contrats fournisseurs ?
- Cyber Crucible fonctionne-t-il aux côtés d'autres outils de cybersécurité et d'EDR ?
- Pourquoi l'IA constitue-t-elle un risque commercial, et non simplement un outil de productivité, pour les dirigeants d'entreprise ?
- Les employés utilisent-ils déjà des outils d'IA avant même que notre entreprise ait mis en place une politique officielle en matière d'IA ?
- Quels sont les signes avant-coureurs d'une attaque par rançongiciel ?
- Que se passe-t-il réellement pendant les instants d'une attaque par ransomware ?
- Que se passe-t-il réellement lorsqu'un rançongiciel attaque un serveur d'entreprise ?
- Pourquoi le rançongiciel attaque-t-il les fichiers partagés avant d'atteindre mon poste de travail ?

- Qu'est-ce qui a inspiré le fondateur à créer Cyber Crucible ?
- D'où proviennent réellement les attaques par rançongiciel ?
- Qui les attaquants de ransomware ciblent-ils réellement aujourd'hui ?
- Qui court le plus grand risque d'une attaque par rançongiciel, et pourquoi ces cibles sont-elles visées ?
- Qui mène réellement les attaques par rançongiciel et comment opèrent-elles ?
- Quel est le client idéal pour la protection contre les rançongiciels de Cyber Crucible ?
- Pourquoi les attaques par rançongiciel deviennent-elles plus fréquentes chaque année ?
- Pourquoi Cyber Crucible utilise-t-il l'IA plutôt qu'une équipe SOC humaine pour arrêter les rançongiciels ?
- Pourquoi les équipes de sécurité reçoivent-elles des milliers d'alertes par jour, et comment peuvent-elles y faire face ?
- Pourquoi le vol d'identifiants et d'identité est-il plus dangereux que le chiffrement par ransomware ?
- Pourquoi le rançongiciel est-il devenu si difficile à arrêter et dont il est si difficile de se remettre ?
- Pourquoi les antivirus traditionnels ne peuvent-ils pas arrêter les attaques de ransomware zero-day et sans fichier ?
- Les pirates utiliseront-ils davantage l'IA dans les attaques par rançongiciel en 2025 ?
- L'utilisation de Cyber Crucible réduit-elle le budget de sécurité global d'une entreprise ?

Les entreprises réagissent-elles de manière excessive face au risque lié à l'IA, ou s'agit-il d'un problème de visibilité ?

Réponse courte : La plupart des organisations ne réagissent pas de manière excessive face au risque lié à l'IA — elles manquent simplement d'une véritable visibilité sur la façon dont les outils d'IA sont réellement utilisés au sein de leur environnement. En l'absence de cette visibilité, l'hypothèse la plus prudente est que le risque actuel est sous-estimé, et non exagéré.

Pourquoi le « risque lié à l'IA » se résume souvent à des angles morts

Lorsque les entreprises évaluent leur exposition au risque lié à l'IA, un schéma récurrent apparaît : certaines organisations reconnaissent ouvertement n'avoir aucune vision claire de la manière dont les outils d'IA sont utilisés en interne. D'autres pensent disposer de cette visibilité, pour découvrir qu'il n'en est rien une fois qu'une surveillance est réellement mise en place. Dans la pratique, dès que le suivi est activé, le volume et la diversité de l'utilisation des outils d'IA qui apparaissent sont souvent surprenants, au point que les fonctionnalités de visibilité doivent parfois être exécutées en mode contrôlé ou simulé, simplement pour suivre le rythme de l'activité qui se manifeste presque immédiatement.

Cet écart suggère que les inquiétudes concernant le risque lié à l'IA sont rarement exagérées. Le plus souvent, ces inquiétudes sont au contraire sous-estimées, car les dirigeants doivent se prononcer sans disposer des données nécessaires pour évaluer la situation avec précision.

Pourquoi un risque inconnu doit être traité comme un risque élevé

Une façon utile d'envisager cette question est de la comparer aux finances personnelles : si vous ne vérifiez jamais le solde de votre compte bancaire, l'hypothèse responsable est de supposer que

vous ne disposez pas de fonds importants, et non l'inverse. La même logique s'applique à l'utilisation de l'IA au sein d'une entreprise. En l'absence de variables concrètes, telles que les outils utilisés, leur fréquence d'utilisation et les personnes qui y ont recours, les organisations n'ont aucune base fiable leur permettant de supposer que le risque est faible. Le comportement responsable par défaut consiste à envisager le pire scénario d'exposition, jusqu'à ce que des données d'utilisation réelles prouvent le contraire.

La tendance de fond derrière l'adoption de l'IA

Chez les utilisateurs, dans les unités d'affaires et au sein même des outils d'IA, de nouveaux cas d'usage, souvent non autorisés, continuent d'apparaître plus rapidement que la gouvernance ne peut suivre. Cette tendance constante indique que la plupart des organisations, quelle que soit leur taille ou leur secteur d'activité, sont encore en train de rattraper leur retard sur la manière dont l'IA est réellement utilisée dans leur environnement. Établir une visibilité claire constitue la première étape indispensable avant de pouvoir évaluer ou gérer avec précision le risque lié à l'IA.

https://player.vimeo.com/video/1176539821?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Pourquoi les modèles traditionnels de SOC peinent-ils face aux cyberattaques à vitesse machine ?

Réponse courte : Les centres opérationnels de sécurité (SOC) traditionnels ont été conçus pour une époque plus lente et plus prévisible du piratage informatique, s'appuyant sur des signatures et une analyse humaine pour détecter les menaces après coup. Les attaquants d'aujourd'hui utilisent des outils automatisés qui évoluent constamment, ce qui oblige les défenses à adopter des approches sans signature et préventives, capables d'agir plus rapidement que l'attaque elle-même.

Comment le paysage des menaces a évolué

Il y a quelques années, les outils malveillants se comportaient de manière relativement cohérente et identifiable. Les équipes de sécurité pouvaient élaborer des méthodes de détection basées sur des schémas connus, car les attaquants ne s'appuyaient pas encore fortement sur l'automatisation pour modifier constamment leurs techniques. Cette approche fonctionnait suffisamment bien pour détecter certaines des menaces les plus sophistiquées de l'époque, y compris des attaques hautement ciblées découvertes il y a plus d'une décennie.

Ce paysage n'existe plus. Les attaquants modernes utilisent l'automatisation pour générer rapidement des variantes de leurs outils, ce qui complique la tâche des systèmes de détection basés sur les signatures pour suivre le rythme. Le temps qu'une nouvelle signature soit identifiée, cataloguée et déployée dans une pile de sécurité, l'attaquant est souvent déjà passé à une nouvelle variante.

Pourquoi les modèles de SOC hérités prennent du retard

Les workflows traditionnels des SOC reposent sur l'identification d'indicateurs connus, puis sur une investigation et une réponse menées par des processus largement manuels ou semi-manuels. Ce modèle suppose que les attaquants agissent à un rythme laissant aux défenseurs le temps d'analyser et de réagir. Lorsque les attaques sont automatisées et peuvent muter en temps réel, cette hypothèse s'effondre, laissant un écart persistant entre le moment où une menace apparaît et celui où elle est traitée.

Ce que les défenses modernes doivent faire à la place

Les outils de sécurité doivent désormais fonctionner sans dépendre uniquement de signatures préalablement connues. Ils doivent plutôt détecter et prévenir directement les comportements malveillants, en agissant à la vitesse de la machine plutôt que d'attendre des cycles d'analyse pilotés par l'humain. La technologie FortressAI de Cyber Crucible repose sur ce principe, en se concentrant sur l'arrêt des tentatives de ransomware, de vol de données et d'usurpation d'identité grâce à une action automatisée et préventive plutôt qu'à une correspondance de signatures a posteriori.

https://player.vimeo.com/video/1182235055?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

À quoi ressemble concrètement une cybersécurité véritablement autonome au quotidien ?

Réponse courte : une véritable sécurité autonome doit sembler routinière et demander peu d'efforts, et non constituer une source constante d'alertes ou d'inquiétude. Si un outil de sécurité exige une attention continue, des ajustements ou des soucis permanents, il ne fonctionne pas de manière autonome.

Pourquoi « l'ennui » est l'objectif

Les équipes de sécurité et le personnel informatique jonglent déjà avec plus de tâches qu'ils ne peuvent raisonnablement en accomplir. Ajouter un outil qui exige des vérifications régulières, un examen manuel des alertes ou des dépannages tard dans la nuit va à l'encontre de l'objectif même de l'automatisation. Une protection autonome efficace doit fonctionner discrètement en arrière-plan, un peu comme un extincteur fixé au mur. La plupart des gens ne pensent à leur extincteur que lorsqu'un inspecteur vient une fois par an confirmer qu'il est chargé et prêt à l'emploi. Le reste du temps, il reste simplement là, remplissant son rôle sans nécessiter d'attention.

C'est le niveau d'exigence que la sécurité autonome devrait atteindre. Elle doit gérer les menaces de manière indépendante, sans détourner le personnel d'autres priorités ni s'ajouter à une liste de tâches déjà longue.

Ce que cela signifie en pratique

Si un produit de sécurité vous oblige à consulter constamment des tableaux de bord, à douter qu'il ait bien détecté une menace, ou à perdre le sommeil en vous demandant s'il fonctionne réellement, il n'est pas véritablement autonome : ce n'est qu'une tâche manuelle supplémentaire présentée sous une autre étiquette. FortressAI de Cyber Crucible repose sur ce principe : détecter et arrêter les ransomwares, le vol de données et les activités d'usurpation d'identité sans nécessiter une supervision humaine constante pour fonctionner correctement.

La mesure du succès ne se résume pas à la quantité d'activité générée par un outil de sécurité ni à la fréquence à laquelle il doit être ajusté. Elle se mesure plutôt à combien peu il est nécessaire d'y penser. Lorsque la sécurité autonome fonctionne comme prévu, elle doit être discrète, fiable et pratiquement invisible jusqu'au moment où elle est réellement nécessaire.

https://player.vimeo.com/video/1190816235?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Les outils d'IA comme ChatGPT peuvent-ils remplacer une équipe humaine de cybersécurité ?

Réponse courte : Non. Les outils d'IA à usage général peuvent soutenir le travail de sécurité en résumant des informations ou en répondant à des questions simples, mais ils ne sont pas suffisamment fiables pour remplacer une équipe de sécurité formée lorsque de véritables décisions liées au risque sont en jeu.

Pourquoi la confiance affichée par l'IA peut être trompeuse

Des outils comme ChatGPT présentent souvent leurs réponses avec un ton d'assurance, même lorsque les informations sous-jacentes sont incomplètes ou incorrectes. Cela peut créer un faux sentiment d'autorité, comparable à celui d'une personne persuasive qui affirme une chose avec suffisamment de conviction pour que les autres l'acceptent comme un fait sans la vérifier davantage. Dans une conversation ordinaire, ce type d'assurance déplacée n'est qu'un problème mineur. En cybersécurité, où les décisions influencent la manière dont une organisation identifie les menaces et y répond, accepter une réponse inexacte sans la remettre en question peut causer un réel préjudice. L'analyse de sécurité repose sur le contexte, la vérification et le jugement, des éléments que les modèles d'IA générale actuels ne sont pas en mesure de reproduire pleinement.

Là où l'IA peut encore aider

Malgré ces limites, les outils d'IA ne sont pas dénués de valeur dans un contexte de sécurité. Ils peuvent servir de point de départ pour la recherche, aider à expliquer des concepts, ou contribuer à la rédaction et à l'organisation d'informations. Utilisée de cette manière, l'IA agit comme un outil de soutien plutôt que comme un décideur. L'essentiel est de reconnaître la différence entre une IA qui assiste un analyste compétent et une IA qui tente d'évaluer et d'atténuer les risques de manière autonome, ce qui exige une expertise plus approfondie que celle offerte actuellement par ces outils.

Pour des attentes honnêtes

Les fournisseurs d'IA et les praticiens qui fixent des attentes réalistes, plutôt que de surestimer ce que ces outils peuvent accomplir, sont plus susceptibles d'instaurer une confiance durable. Survendre les capacités de l'IA en matière de sécurité risque d'éroder la confiance une fois que les limites deviennent évidentes. Une communication claire et mesurée sur ce que l'IA peut et ne peut pas faire aide les organisations à faire des choix éclairés quant à la manière de l'intégrer de façon responsable. L'approche de Cyber Crucible reflète ce même principe : plutôt que de présenter l'IA comme un substitut à des défenseurs compétents, les technologies de protection autonomes comme FortressAI sont conçues pour fonctionner aux côtés de l'expertise humaine, renforçant la capacité d'une organisation à prévenir les rançongiciels, le vol de données et l'usurpation d'identité, sans prétendre éliminer le besoin d'une supervision éclairée.

https://player.vimeo.com/video/1134578207?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Les rançongiciels peuvent-ils toujours atteindre les données stockées dans des services cloud comme OneDrive ou Google Drive ?

Réponse courte : Oui. Si le stockage cloud était autrefois hors de portée des rançongiciels, les attaquants ont adapté leurs méthodes et peuvent désormais cibler les données stockées dans le cloud grâce à des techniques telles que le mappage de lecteurs et, plus couramment aujourd'hui, le vol de clés API et de jetons de session.

Comment l'approche des rançongiciels vis-à-vis des données cloud a évolué

Lorsque le travail à distance a entraîné une transition rapide vers le stockage cloud, les entreprises comme les cybercriminels se sont adaptés simultanément à ce nouvel environnement. Aux premiers stades de cette transition, les rançongiciels ne pouvaient généralement pas atteindre les fichiers stockés sur des plateformes cloud — si les données se trouvaient dans le cloud plutôt que sur un serveur local, les attaquants les laissaient généralement de côté car ils ne disposaient d'aucun accès direct à celles-ci.

Cette situation a changé lorsque les attaquants ont appris à connecter manuellement un stockage cloud, tel qu'un compte Amazon, OneDrive ou Google Drive, à un système infecté. Ils procédaient en montant le stockage cloud sous forme de lettre de lecteur local, de manière similaire à un périphérique USB apparaissant comme un lecteur distinct sur un ordinateur. Une fois monté de cette façon, les fichiers hébergés dans le cloud devenaient tout aussi exposés au chiffrement que les fichiers présents sur un disque dur local.

La menace la plus importante aujourd'hui : le vol de clés et de jetons

À mesure que l'utilisation du cloud a mûri, les tactiques des attaquants ont de nouveau évolué. Plutôt que de monter manuellement des lecteurs, beaucoup s'attaquent désormais aux clés API et aux jetons de session — des identifiants qui accordent un accès direct, au niveau applicatif, aux comptes et aux données du cloud. Obtenir l'un de ces éléments équivaut à voler un mot de passe, si ce n'est que cela offre souvent un accès plus large et plus rapide aux ressources cloud qu'un simple mot de passe volé.

Cette évolution est importante car la même rapidité et la même évolutivité qui rendent l'informatique en nuage précieuse pour les équipes informatiques légitimes sont désormais également à la disposition des attaquants. Parmi les clients de Cyber Crucible l'année dernière, plus de la moitié ont subi une tentative de vol de jeton de session cloud visant à détourner la session active d'un utilisateur, tandis que moins de 9 % ont constaté une compromission réelle de données. Cela suggère que les attaquants privilégient le vol d'identifiants et de jetons comme point d'entrée principal, le vol de données étant un objectif secondaire.

Les données stockées dans le cloud sont-elles automatiquement en sécurité ?

Le stockage cloud ne garantit pas une protection contre les rançongiciels ou le vol de données. Il modifie simplement la méthode que les attaquants doivent employer pour atteindre ces données — déplaçant le risque principal vers la compromission des identifiants et des jetons de session plutôt que vers le chiffrement direct des fichiers.

https://player.vimeo.com/video/1047006345?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Si un rançongiciel s'autodétruit, cela signifie-t-il que l'attaque est terminée ?

Réponse courte : Non. Les rançongiciels modernes sont souvent conçus pour s'effacer une fois qu'ils ont terminé le chiffrement des fichiers, mais cette autodestruction n'a aucun rapport avec la question de savoir si vos systèmes ou vos données sont réellement en sécurité — elle ne fait qu'effacer les preuves de l'outil qui a causé les dégâts.

Pourquoi la « disparition » du rançongiciel ne signifie pas la récupération

Les attaquants d'aujourd'hui s'appuient rarement sur un seul logiciel malveillant pour mener toute une intrusion. Ils utilisent généralement une séquence d'outils distincts : l'un pour collecter des identifiants, un autre pour localiser et exfiltrer des données précieuses, et un dernier pour chiffrer les fichiers afin d'obtenir un maximum de levier de pression. Une fois que ce dernier outil de chiffrement a terminé sa tâche, il s'efface couramment lui-même du système. Ce qui reste, ce sont des notes de rançon contenant des instructions de contact et, plus important encore, des fichiers qui demeurent verrouillés. L'absence du logiciel malveillant lui-même n'est pas un signe de résolution — cela signifie simplement que la tâche de l'attaquant est terminée, de son point de vue.

Ce qui arrive réellement à vos données

Au moment où le chiffrement a lieu, tout vol de données a généralement déjà eu lieu, et ces informations sont perdues quoi qu'il arrive par la suite. Les fichiers chiffrés qui subsistent peuvent, dans certains cas, être traités par la négociation avec l'attaquant ou par des outils de déchiffrement, mais il n'existe aucune garantie de succès. Les techniques qui permettaient autrefois un déchiffrement automatisé sans payer les attaquants sont devenues beaucoup moins efficaces à mesure que les opérateurs de rançongiciels ont adapté leurs méthodes. Il n'existe aucune action de récupération simple, telle que le redémarrage d'un appareil, qui puisse inverser le chiffrement.

Le véritable choix après une attaque

Une fois que le rançongiciel a accompli son œuvre et s'est autodétruit, les organisations disposent généralement de deux options : reconstruire les systèmes et les données affectés à partir de sauvegardes saines, ou tenter un déchiffrement en payant et en négociant avec l'attaquant. Aucune de ces options n'est rapide ni garantie, c'est pourquoi la prévention — arrêter le rançongiciel avant que le chiffrement et le vol de données ne se produisent — demeure bien plus efficace que de tenter de réagir après coup.

https://player.vimeo.com/video/1043482941?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

La cybersécurité doit-elle se concentrer sur la résilience ou sur la prévention des attaques dès le départ ?

Réponse courte : La résilience — se rétablir après une attaque — a de l'importance, mais l'objectif le plus important est de prévenir les rançongiciels, le vol de données et l'usurpation d'identité avant que des dommages ne surviennent, car les attaques automatisées sont incessantes et de plus en plus bien informées sur le moment opportun pour frapper.

Deux significations de la « résilience »

Le terme « résilience » en cybersécurité a évolué vers deux idées différentes. La première est de savoir si vos outils de sécurité eux-mêmes peuvent continuer à fonctionner sous une attaque — c'est-à-dire si le logiciel censé vous protéger peut survivre à une attaque ou à une tentative de sabotage directe, un peu comme se demander si une caméra de sécurité peut continuer à enregistrer après qu'on ait tenté de la désactiver. L'autre signification, plus traditionnelle, est de savoir si votre entreprise peut se rétablir et rebondir après qu'une violation s'est déjà produite.

Les deux comptent, mais aucune ne devrait constituer la stratégie principale. Les attaques modernes sont automatisées et constantes. La principale raison pour laquelle les organisations ne sont pas frappées sans relâche est que les attaquants sont devenus experts dans la lecture des signaux indiquant quelles cibles valent la peine d'être visées — par exemple, en évitant les entreprises qui n'ont manifestement pas les ressources financières permettant de rendre une attaque rentable. Ce niveau de ciblage automatisé signifie que la résilience seule constitue une posture réactive face à un adversaire qui sonde en permanence.

Pourquoi la prévention doit venir en premier

Être résilient après une violation est comparable au fait d'avoir un bon garage de réparation à disposition après un accident de voiture. C'est utile, mais il est bien préférable d'éviter complètement l'accident. Personne ne veut tester l'efficacité du processus de réparation s'il peut

plutôt éviter la collision dès le départ.

Appliqué à la sécurité des entreprises, cela signifie que la priorité doit être d'arrêter les attaques avant qu'elles ne réussissent — l'équivalent d'avoir des freins fiables plutôt qu'un simple bon plan de réparation après un accident. Cyber Crucible œuvre en ce sens en se concentrant sur la prévention autonome, avec pour objectif d'arrêter les tentatives de rançongiciel, de vol de données et d'usurpation d'identité avant qu'elles ne puissent causer des dommages, plutôt que de dépendre uniquement du rétablissement et du nettoyage après coup.

https://player.vimeo.com/video/1194994916?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Comment Cyber Crucible m'aide-t-il à gérer les fournisseurs de cybersécurité et les résultats ?

Réponse courte : Cyber Crucible gère la prévention automatisée au niveau du terminal, ce qui vous libère pour sélectionner et tenir responsable votre propre fournisseur de surveillance ou de réponse, plutôt que d'être enfermé dans un service groupé et difficile à évaluer, lié à un seul fournisseur d'EDR ou de XDR.

Le problème caché des services de sécurité groupés

De nombreuses organisations paient des sommes importantes pour un centre d'opérations de sécurité hébergé qui est associé à un produit particulier de détection ou de détection et réponse étendues au niveau des terminaux. Le problème est que cet arrangement laisse souvent le client avec peu de visibilité sur l'attention ou l'efficacité réelle de ce service de surveillance. Vous ne savez peut-être pas à quel point votre environnement est surveillé de près, à quelle vitesse les incidents sont escaladés, ou si vous êtes un compte prioritaire pour ce fournisseur. Comme la surveillance est liée à la technologie sous-jacente, il y a peu de marge de négociation, de mesure ou de remplacement du service s'il ne répond pas aux attentes.

Séparer la prévention de la surveillance redonne le contrôle

Cyber Crucible se concentre sur la couche de prévention de la protection des terminaux, en arrêtant automatiquement les tentatives de ransomware, de vol de données et d'usurpation d'identité. Comme la prévention est gérée de manière indépendante, les organisations ne sont plus contraintes d'accepter une offre groupée unique pour la détection et la réponse. Au lieu de cela, vous avez la liberté de choisir le partenaire de détection et réponse gérées (MDR) ou de services de sécurité gérés (MSSP) qui répond à vos besoins, qu'il s'agisse de votre propre personnel interne,

d'un MSSP spécialisé, ou d'un tout autre fournisseur de MDR.

Pourquoi le choix est important

Cette séparation vous donne la possibilité de définir vos propres accords de niveau de service, de mesurer la qualité et la réactivité de l'équipe qui surveille votre environnement, et de tenir ce fournisseur responsable par le biais d'une véritable relation contractuelle. Plutôt que d'espérer qu'un fournisseur groupé vous accorde une attention adéquate, vous pouvez évaluer et faire respecter des normes de performance selon vos propres critères. En fin de compte, l'approche de Cyber Crucible vise à donner aux organisations un contrôle véritable — un contrôle face aux attaquants, et tout aussi important, un contrôle sur les relations avec les fournisseurs et les contrats qui soutiennent leur programme de sécurité.

https://player.vimeo.com/video/1046829518?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Comment Cyber Crucible m'aide-t-il à maîtriser mes dépenses de cybersécurité et mes contrats fournisseurs ?

Réponse courte : Cyber Crucible ne réduit pas nécessairement votre budget total de sécurité, mais il vous donne davantage de contrôle sur la manière dont ce budget est dépensé en vous permettant de dissocier la prévention des ransomwares et du vol de données de la surveillance et des services de réponse — vous pouvez ainsi choisir et tenir responsable le fournisseur qui gère cette dernière.

Le coût caché des services SOC groupés

De nombreuses organisations versent des sommes importantes à un centre opérationnel de sécurité (SOC) hébergé, fourni conjointement avec une plateforme EDR ou XDR. Le problème de ce type d'arrangement est que le client dispose généralement de peu de visibilité sur l'attention réelle et l'efficacité de cette équipe de surveillance. Il n'existe aucun moyen simple de mesurer la qualité de la réponse, l'engagement du personnel, ou le degré de priorité réellement accordé à votre compte. Vous faites essentiellement confiance au fait que le service en coulisses fonctionne bien, sans moyen pratique de le vérifier.

Dissocier la prévention de la surveillance

Cyber Crucible se concentre spécifiquement sur le volet prévention de la protection des points de terminaison — arrêter les ransomwares, le vol de données et l'usurpation d'identité avant que des dommages ne surviennent. Étant donné que la prévention est gérée de manière indépendante, les organisations ne sont plus enfermées dans un fournisseur unique regroupant à la fois la prévention et la surveillance. Cela signifie que vous pouvez sélectionner votre propre fournisseur de détection et de réponse gérées (MDR), votre MSSP, ou même vous appuyer sur votre équipe interne pour

assurer la surveillance et la réponse continues.

Reprendre le contrôle sur la responsabilité des fournisseurs

Cette dissociation est importante car elle vous redonne la capacité de négocier et de faire respecter des accords de niveau de service clairs avec les fournisseurs que vous choisissez. Vous pouvez évaluer la réactivité, mesurer la performance et tenir les prestataires responsables, ce qui n'est pas possible lorsque prévention et surveillance sont liées ensemble dans un seul et même contrat. En résumé, la valeur ne réside pas uniquement dans la défense technique contre les attaquants — elle réside aussi dans le fait de reprendre la supervision et le contrôle de vos propres relations fournisseurs, de vos contrats et de la qualité du service pour lequel vous payez.

https://player.vimeo.com/video/1046667196?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Cyber Crucible fonctionne-t-il aux côtés d'autres outils de cybersécurité et d'EDR ?

Réponse courte : Oui. Cyber Crucible est construit sur ses propres capteurs propriétaires et sa propre technologie de surveillance comportementale, ce qui lui permet de fonctionner aux côtés de pratiquement n'importe quel autre produit de sécurité sans interférer avec les outils existants.

Pourquoi la compatibilité ne pose pas de problème

Cyber Crucible ne s'appuie pas sur des points d'ancrage EDR partagés ni sur des intégrations au niveau système dont dépendent également d'autres éditeurs de sécurité. Comme son approche de détection et de surveillance, y compris les méthodes de collecte comportementale qui sous-tendent FortressAI, est conçue sur mesure depuis la base, elle n'entre pas en concurrence pour les mêmes ressources système et n'interfère pas avec les points d'ancrage utilisés par d'autres outils de protection des points d'accès. Cette conception permet à Cyber Crucible de fonctionner comme une couche de protection supplémentaire plutôt que comme un remplacement ou une superposition conflictuelle. Il a été déployé aux côtés de produits d'un large éventail d'éditeurs de sécurité reconnus, et dans la pratique, la plupart des environnements ne présentent aucun problème de compatibilité.

Quand des ajustements sont nécessaires

La situation rare qui nécessite une configuration supplémentaire concerne les logiciels internes personnalisés qu'une entreprise a développés en interne. Il arrive occasionnellement que ces outils maison présentent des schémas de comportement qui ressemblent au type d'activité que Cyber Crucible est conçu pour détecter, comme des modifications rapides de fichiers ou des interactions système inhabituelles. Lorsque cela se produit, la solution est simple : une règle d'exclusion peut être ajoutée pour que Cyber Crucible reconnaisse l'outil interne comme légitime. Cette exclusion reste fiable tant que le logiciel interne demeure correctement signé et non modifié, c'est-à-dire qu'il continue de correspondre à son état attendu et vérifié. Si ces conditions sont respectées,

l'outil fonctionne normalement aux côtés de Cyber Crucible sans friction continue.

Ce que cela signifie pour les équipes de sécurité

Les organisations n'ont pas besoin de supprimer ou de reconfigurer leur dispositif de sécurité actuel pour adopter Cyber Crucible. Il est conçu pour compléter les défenses existantes, en ajoutant une couche dédiée axée sur la prévention des rançongiciels, du vol de données et de l'usurpation d'identité, sans perturber les outils qui protègent déjà l'environnement.

https://player.vimeo.com/video/1043463490?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Pourquoi l'IA constitue-t-elle un risque commercial, et non simplement un outil de productivité, pour les dirigeants d'entreprise ?

Réponse courte : Les équipes dirigeantes considèrent souvent l'IA uniquement comme un outil d'amélioration de la productivité, mais une utilisation non maîtrisée de l'IA peut exposer directement à des tiers extérieurs des secrets commerciaux essentiels — plans produits, données de chiffre d'affaires et stratégie commerciale. Il s'agit d'un risque stratégique et financier qui concerne le PDG, le directeur financier, le directeur des opérations et la direction commerciale, et pas uniquement le service informatique.

Un type d'exposition différent

Les incidents traditionnels de cybersécurité, comme une violation de données qui expose des dossiers clients sur le dark web, suivent un schéma familier : la direction réagit, les régulateurs peuvent intervenir, des amendes sont parfois payées, et le conseil d'administration reçoit un compte-rendu. Les entreprises ont déjà géré ce type de situation, et des processus existent pour la traiter.

L'IA introduit une nouvelle catégorie d'exposition, moins bien comprise. Lorsque les employés utilisent des outils d'IA sans garanties appropriées, ils peuvent transmettre des informations commerciales confidentielles — plans de produits futurs, prévisions de bénéfices, pipelines de ventes — à des systèmes qui n'ont jamais été conçus pour garder ces informations confinées. Contrairement à un incident de piratage, cela ne résulte pas nécessairement d'une attaque. Cela peut se produire simplement par une utilisation normale et bien intentionnée de l'IA par le personnel.

Le problème des requêtes internes

Un risque souvent négligé concerne ce qui se passe en interne au sein d'une entreprise dès lors qu'un outil d'IA dispose d'un accès étendu aux documents et données internes. Si les contrôles d'accès ne sont pas soigneusement conçus, un employé pourrait poser une simple question à un assistant IA et recevoir une réponse détaillée contenant des plans sensibles qui ne devraient jamais circuler librement, même en interne. Il s'agit d'une défaillance de gouvernance, et non d'un simple problème technique, qui peut s'avérer tout aussi dommageable qu'une fuite externe.

Pourquoi cela relève de la direction

Le choix de ne pas investir dans un environnement d'IA interne correctement contrôlé n'élimine pas cette catégorie de risque ; il ne fait que la déplacer en dehors du périmètre de supervision directe de l'organisation. Les dirigeants d'entreprise n'envisageraient jamais de publier des comptes de résultats ou des pipelines de ventes sur un site web public. Une utilisation non maîtrisée de l'IA peut créer un résultat similaire sans que personne ne l'ait voulu. Traiter cette question comme un risque commercial essentiel, plutôt que comme un simple problème technique, est indispensable pour protéger les avantages concurrentiels que la direction s'est efforcée de construire.

https://player.vimeo.com/video/1211538534?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Les employés utilisent-ils déjà des outils d'IA avant même que notre entreprise ait mis en place une politique officielle en matière d'IA ?

Réponse courte : Oui. La plupart des organisations découvrent que les employés, sous-traitants, consultants et fournisseurs utilisent déjà des outils d'IA de manière créative et parfois inattendue, bien avant qu'une politique ou un projet de gouvernance en matière d'IA officiel ne soit finalisé. Attendre une politique « parfaite » avant de traiter l'usage de l'IA laisse une entreprise aveugle face à ce qui se passe déjà.

L'hypothèse courante

De nombreux dirigeants supposent que l'adoption de l'IA au sein de leur organisation est suspendue jusqu'à ce qu'une politique officielle soit rédigée, approuvée et déployée. Selon ce raisonnement, les employés attendraient patiemment des règles claires avant d'expérimenter de nouveaux outils. En pratique, cette hypothèse se vérifie rarement. Les personnes ont tendance à chercher des moyens de travailler plus efficacement, que des directives formelles existent déjà ou non.

Ce que les organisations constatent réellement

Lorsque les entreprises mettent en place des outils de surveillance ou d'application des règles, tels que FortressAI de Cyber Crucible, elles découvrent souvent que l'usage de l'IA est bien plus répandu et varié que prévu. Le personnel fait naturellement preuve de débrouillardise ; cette même créativité et cet esprit de résolution de problèmes qui font d'eux des employés précieux les conduisent également à trouver de nouvelles façons non autorisées d'utiliser des outils d'IA pour gagner du temps ou améliorer leur production. Il ne s'agit pas tant d'un signe de mauvaise intention que de la nature humaine : les gens utiliseront les outils disponibles pour faciliter leur

travail, qu'une politique le permette officiellement ou non.

Pourquoi la visibilité compte plus qu'une politique parfaite

Le véritable risque n'est pas qu'une politique n'ait pas encore été finalisée. C'est que les organisations manquent souvent de visibilité sur la manière dont l'IA est déjà utilisée dans leur environnement. Sans cette visibilité, les équipes de sécurité et de conformité ne peuvent pas évaluer l'exposition aux fuites de données, à l'utilisation non autorisée d'outils, ou à d'autres risques liés à l'adoption de l'IA. Plutôt que d'attendre l'achèvement d'un cadre de gouvernance de l'IA complet, les organisations ont intérêt à d'abord obtenir un aperçu des tendances d'usage actuelles. Comprendre ce qui se passe réellement sur le terrain permet d'établir des politiques ancrées dans la réalité plutôt que sur des suppositions concernant le comportement des employés.

https://player.vimeo.com/video/1176537677?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Quels sont les signes avant-coureurs d'une attaque par rançongiciel ?

Réponse courte : Une fois qu'un rançongiciel est déclenché, il peut paralyser une entreprise en aussi peu que 60 à 90 secondes. Les signes avant-coureurs visibles ont donc tendance à n'apparaître qu'une fois l'attaque déjà en cours, et non suffisamment à l'avance pour l'arrêter manuellement. La véritable défense consiste à détecter le travail de préparation que les attaquants effectuent en amont, avant même qu'ils ne déclenchent l'action finale.

Pourquoi un rançongiciel semble soudain

Les attaques par rançongiciel sont souvent décrites comme instantanées, mais cela est trompeur. Les attaquants passent généralement du temps à l'intérieur d'un réseau au préalable, cartographiant discrètement les systèmes, obtenant des accès et se positionnant pour causer un maximum de dégâts. Ce travail de fond s'apparente à celui d'une équipe militaire préparant un champ de bataille avant le début d'une opération. Une fois que tout est en place, l'événement de chiffrement ou de verrouillage proprement dit peut se dérouler en moins de deux minutes. Le temps que les employés remarquent qu'un problème existe, les dégâts sont déjà largement engagés.

À quoi ressemble le moment de l'attaque

Lorsqu'une attaque s'exécute, les entreprises constatent souvent un changement soudain et troublant : certaines applications ou services cessent de répondre, les connexions réseau deviennent instables, les systèmes téléphoniques peuvent tomber en panne, et les opérations normales semblent perturbées presque simultanément. Tout aussi inquiétant, certains systèmes continuent de fonctionner normalement pendant cette période. Cette apparente normalité n'est pas bon signe. Elle signifie souvent que les attaquants utilisent ces systèmes non touchés comme couverture pendant que le reste de l'environnement est compromis.

Pourquoi la détection précoce compte plus que la réaction

Étant donné que les signes visibles d'un rançongiciel n'apparaissent que dans les dernières secondes, rapides, d'une attaque, attendre de réagir à ces signes n'est pas une stratégie fiable. Une protection significative dépend de l'identification et de l'arrêt de l'activité malveillante dès le stade de préparation, avant que les attaquants ne soient prêts à agir. C'est à ce niveau que des outils de détection autonomes comme FortressAI de Cyber Crucible sont conçus pour opérer, visant à interrompre le comportement des attaquants avant qu'il n'atteigne le point de non-retour, plutôt que d'attendre les symptômes extérieurs qui apparaissent une fois l'attaque déjà en cours.

https://player.vimeo.com/video/1043488930?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Que se passe-t-il réellement pendant les instants d'une attaque par ransomware ?

Réponse courte : La phase de chiffrement proprement dite d'une attaque par ransomware est remarquablement rapide, se terminant souvent en environ 60 à 90 secondes une fois déclenchée, bien que les attaquants passent un temps considérable et invisible en amont à se positionner à l'intérieur du réseau. Au moment où les symptômes visibles apparaissent, les dégâts sont déjà en train de se produire en temps réel, c'est pourquoi la détection doit intervenir avant le déclenchement final, et non après.

Le calme avant l'attaque

Avant que le ransomware ne s'active, les attaquants passent généralement du temps à se déplacer discrètement dans les systèmes de l'entreprise, à identifier les données précieuses, à désactiver les sauvegardes et à mettre en place les conditions nécessaires à une attaque réussie. Ce travail préparatoire peut passer inaperçu, car les opérations commerciales normales se poursuivent comme d'habitude. Le réseau peut sembler stable et sain jusqu'au moment où l'attaquant décide de lancer la phase finale. Un peu comme le silence inquiétant qui précède une catastrophe, cette période de calme peut être trompeuse, car elle ne reflète pas la perturbation qui est sur le point de se produire.

L'apparition rapide des dégâts

Une fois lancé, un événement de ransomware peut se dérouler en moins de deux minutes. Dans cette courte fenêtre, les employés peuvent remarquer des pannes soudaines : les e-mails cessent de fonctionner, les systèmes téléphoniques deviennent silencieux, les applications se comportent de manière erratique ou les connexions réseau deviennent instables. Ce sont des symptômes du chiffrement et de la compromission des systèmes se produisant simultanément dans l'ensemble de l'environnement. Comme le processus se déroule si rapidement, il n'y a généralement pas assez de temps pour qu'une personne intervienne manuellement une fois qu'il a commencé.

Pourquoi certains systèmes continuent de fonctionner

Un détail troublant de nombreux incidents de ransomware est que tout ne tombe pas en panne en même temps. Certains services peuvent continuer à fonctionner normalement alors que d'autres s'effondrent. Cela s'explique souvent par le fait que ces systèmes non affectés sont précisément l'endroit où l'attaquant opère encore, les utilisant comme point d'ancrage ou zone de préparation. Reconnaître ce schéma est important, car supposer qu'un problème n'est « que partiel » peut créer un faux sentiment de sécurité alors que la compromission est activement en cours. Une prévention efficace dépend de l'identification et de l'arrêt de l'activité malveillante avant que la phase destructrice finale ne commence, car une fois déclenchée, la fenêtre d'action est extrêmement courte.

https://player.vimeo.com/video/1046658956?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Que se passe-t-il réellement lorsqu'un rançongiciel attaque un serveur d'entreprise ?

Réponse courte : Lorsqu'un rançongiciel frappe un serveur, les attaquants désactivent généralement d'abord ses services, puis chiffrent ses données tout en empêchant les équipes informatiques et de sécurité d'intervenir — utilisant parfois des dizaines, voire des centaines de postes de travail compromis pour effectuer le chiffrement à distance.

Les premiers signes d'une attaque

L'un des premiers indicateurs qu'un serveur a été compromis est une perte soudaine de service. Comme les attaquants savent que le rançongiciel peut accidentellement corrompre des fichiers en cours de chiffrement, beaucoup arrêtent délibérément les applications s'exécutant sur un serveur avant que le processus de chiffrement ne commence. Cela signifie que les employés ou les clients dépendant de ce système — qu'il s'agisse d'une plateforme de paie, d'une application web ou d'un autre service critique pour l'entreprise — peuvent constater une interruption de service avant même que quiconque ne réalise qu'un incident de sécurité est en cours.

Bloquer les défenseurs pendant que le chiffrement se propage

Une fois l'attaque en cours, le rançongiciel commence à chiffrer les données stockées sur le serveur. Pour empêcher les équipes de sécurité ou les administrateurs d'intervenir, les attaquants bloquent fréquemment l'accès réseau au serveur, l'isolant des personnes qui répondraient normalement à la menace. Cette tactique donne à l'attaquant le temps de terminer le chiffrement des fichiers avant que les défenseurs ne puissent agir.

Les postes de travail peuvent être le véritable point faible

Il est intéressant de noter que le serveur lui-même n'est pas toujours à l'origine du danger. Dans de nombreux cas, les attaquants compromettent un grand nombre de postes de travail des employés — parfois 50, 70 ou plus — qui disposent déjà d'un accès légitime au serveur. Ces postes de travail sont ensuite utilisés simultanément pour chiffrer à distance les données du serveur. Comme l'attaque est lancée depuis plusieurs terminaux à la fois, les postes de travail connectés au serveur représentent souvent une vulnérabilité plus importante que l'infrastructure du serveur elle-même.

Ce schéma illustre pourquoi la défense contre les rançongiciels ne peut pas se concentrer uniquement sur les serveurs. La sécurité des terminaux, sur chaque appareil ayant accès au serveur, joue un rôle essentiel pour arrêter les attaques avant que le chiffrement ne se propage. FortressAI de Cyber Crucible est conçu pour identifier et interrompre ces comportements dès les premiers stades, que la menace provienne d'un serveur ou se propage à partir de postes de travail connectés.

https://player.vimeo.com/video/1041172405?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Pourquoi le rançongiciel attaque-t-il les fichiers partagés avant d'atteindre mon poste de travail ?

Réponse courte : Lorsqu'un rançongiciel infecte un poste de travail individuel, cette machine est rarement la cible réelle. Les attaquants utilisent l'infection initiale comme point de lancement pour atteindre les ressources réseau partagées, et ils ne chiffrent ou n'endommagent le poste de travail local qu'après s'être déjà attaqués à des données de plus grande valeur ailleurs.

Pourquoi le poste de travail est le dernier arrêt, pas le premier

Une idée reçue courante est que si un rançongiciel atteint l'ordinateur d'un employé donné, ce sont les fichiers de cet employé que les attaquants recherchent. En réalité, le logiciel malveillant est programmé pour dépasser la machine locale presque immédiatement. Une fois qu'il obtient un point d'ancrage, il commence à analyser le réseau à la recherche de ressources accessibles de plus grande valeur, telles que des serveurs de fichiers, des wikis internes ou des bases de données contenant des informations sur les clients. Le chiffrement ou l'exfiltration de ces données centralisées constitue le véritable objectif, car cela affecte une bien plus grande partie de l'organisation que le dossier d'un seul utilisateur.

La note de rançon arrive en dernier, pas en premier

Étant donné que les attaquants privilégient les données à l'échelle du réseau avant de toucher l'appareil d'origine, l'employé infecté est généralement la dernière personne à remarquer un problème. Au moment où une note de rançon apparaît sur son écran, les attaquants ont généralement déjà terminé de chiffrer ou de voler des données à travers une grande partie de l'infrastructure de l'entreprise. Cet ordonnancement est intentionnel. Il permet aux attaquants d'infliger un dommage opérationnel maximal avant que quiconque au sein de l'organisation n'ait la

possibilité de détecter l'intrusion ou d'y répondre. La note de rançon visible n'est essentiellement qu'un signal indiquant que les dommages les plus graves se sont déjà produits en coulisses.

Ce que cela signifie pour la défense

Les photos ou documents personnels stockés localement sur un poste de travail constituent généralement la cible la moins importante lors d'une attaque par rançongiciel, même s'ils peuvent en être le signe le plus visible. Une défense efficace doit tenir compte de ce schéma en se concentrant sur la détection et l'arrêt de l'activité malveillante le plus tôt possible, avant qu'elle ne puisse atteindre les systèmes partagés. FortressAI de Cyber Crucible a été conçu en tenant compte de cette séquence d'attaque, visant à intervenir dès les premières étapes d'une intrusion plutôt que de réagir uniquement une fois que le chiffrement devient visible sur les machines individuelles.

https://player.vimeo.com/video/1043466243?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Qu'est-ce qui a inspiré le fondateur à créer Cyber Crucible ?

Réponse courte : Cyber Crucible est né d'une carrière consacrée à la conception de solutions sur mesure pour des missions gouvernementales classifiées, et d'une volonté de mettre cette même capacité à résoudre des problèmes au service d'un bien plus grand nombre de personnes, afin de les aider à lutter contre les rançongiciels et la cybercriminalité dans le monde entier.

Des missions classifiées à un problème mondial

Bien avant que Cyber Crucible n'existe en tant qu'entreprise, son fondateur résolvait déjà des problèmes de sécurité complexes, allant jusqu'à identifier un moyen de prendre le contrôle d'un botnet afin d'en protéger les personnes visées. Cette habitude de décomposer des défis techniques ardus et de concevoir des solutions concrètes s'est poursuivie tout au long d'une carrière au sein de la National Security Agency et d'autres organisations gouvernementales. À maintes reprises, un nouvel outil ou une nouvelle technique était conçu pour répondre à un besoin opérationnel précis, avant d'être utilisé une seule fois, transmis à une équipe alliée, ou mis de côté une fois son objectif restreint atteint. Chaque invention avait son importance, mais son impact s'arrêtait aux frontières d'une seule mission classifiée.

Transformer des solutions isolées en un outil accessible à tous

Ce cycle consistant à résoudre un problème pour ensuite constater que son utilité restait limitée à une seule équipe ou à une seule opération a fini par devenir frustrant, même si le travail en lui-même avait du sens. Lorsque les rançongiciels sont apparus comme une menace généralisée, ils ont représenté une opportunité différente : celle d'appliquer cette même approche inventive, mais cette fois pour répondre à un problème touchant des organisations et des individus partout dans le monde, et non plus une seule unité spécialisée. Le constat était clair : aider une population plus large de personnes exigeait davantage qu'un nouvel outil sur mesure conçu pour un usage restreint. Cela nécessitait un produit commercial capable d'être déployé facilement et de manière

fiable, à grande échelle.

Pourquoi cela façonne Cyber Crucible aujourd'hui

Ce changement de perspective constitue le fondement de l'approche de Cyber Crucible. Plutôt que de concevoir une solution pour une seule équipe ou une seule mission, l'objectif est de créer une technologie, propulsée par FortressAI, qui fonctionne automatiquement et de manière constante pour des organisations partout dans le monde, afin que moins de personnes subissent les dommages et les perturbations causés par les rançongiciels, le vol de données et l'usurpation d'identité. Le travail axé sur des missions du passé garde toute son importance, mais la finalité qui anime Cyber Crucible est d'atteindre et de protéger le plus grand nombre de personnes possible.

https://player.vimeo.com/video/1046673820?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

D'où proviennent réellement les attaques par rançongiciel ?

Réponse courte : les opérateurs de rançongiciels ne se limitent pas à une poignée de pays bien connus ; l'automatisation et les outils criminels bon marché permettent désormais aux attaquants d'opérer depuis presque n'importe où dans le monde.

Le récit médiatique simplifié ne correspond pas aux faits

La couverture médiatique désigne souvent un seul pays ou une seule région comme source des attaques par rançongiciel, car cela permet de produire un titre rapide et facile à assimiler. En pratique, l'expérience directe acquise en répondant à des incidents en cours raconte une histoire bien plus complexe. Lorsque Cyber Crucible a commencé à traiter des cas actifs de rançongiciels, notre équipe a reçu un large éventail d'appels téléphoniques liés aux attaques — beaucoup provenant de téléphones prépayés ou jetables, sans historique de propriété traçable. Ces appels provenaient de nombreuses régions différentes, notamment l'Asie du Sud, le Moyen-Orient, certaines parties de l'Europe, l'Amérique du Sud, et même l'Amérique du Nord. Certains appelants étaient des opérateurs de bas niveau, tandis que d'autres semblaient être les véritables développeurs du logiciel malveillant, engageant parfois des conversations étonnamment professionnelles, d'égal à égal, sur les détails techniques de leurs attaques.

L'automatisation a abaissé la barrière à l'entrée

Bien que certaines régions du monde puissent encore produire une part disproportionnée de développeurs de rançongiciels compétents, l'essor des kits de rançongiciel-service, des outils d'automatisation et des démarches de base assistées par l'IA a considérablement facilité la participation d'acteurs moins sophistiqués. Une personne disposant de compétences techniques limitées peut désormais louer une infrastructure d'attaque, acheter un accès réseau volé auprès de courtiers en accès initial, et mener une campagne d'extorsion avec un investissement initial minimal. Cela a effectivement ouvert la porte à des criminels opportunistes situés n'importe où pour y participer, plutôt que de restreindre l'activité des rançongiciels à un petit groupe lié à des États-nations.

Pourquoi cela compte pour la défense

L'argot régional, les tournures linguistiques et les comportements d'appel observés lors de ces incidents confirment que les attaquants sont géographiquement diversifiés, et non limités à une seule nation « acteur malveillant ». Comprendre les rançongiciels comme une entreprise criminelle mondialement répartie et portée par l'automatisation — plutôt que comme un simple récit géopolitique — permet d'élaborer des stratégies de défense mieux informées et d'obtenir une image plus claire du risque réel auquel les organisations sont confrontées.

https://player.vimeo.com/video/1047715735?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Qui les attaquants de ransomware ciblent-ils réellement aujourd'hui ?

Réponse courte : Les opérateurs de ransomware ne se concentrent plus uniquement sur les grandes organisations très en vue. L'automatisation et les outils pilotés par l'IA ont rendu rentable le ciblage d'entreprises de presque toutes tailles, ce qui signifie que la plupart des organisations doivent partir du principe qu'elles constituent une cible potentielle.

Comment le ciblage a évolué depuis 2020

Aux débuts du ransomware moderne, mener une attaque depuis l'accès initial jusqu'à l'extorsion nécessitait des hackers qualifiés et expérimentés travaillant en grande partie de manière manuelle. Cela limitait le nombre d'attaquants réellement compétents et concentrait l'attention sur les grandes cibles à forte valeur, pour lesquelles le gain justifiait l'effort.

À mesure que la demande augmentait, les groupes de hackers établis ont commencé à fonctionner davantage comme des entreprises en croissance. Plutôt que de dépendre uniquement d'un petit nombre d'opérateurs d'élite, ils ont commencé à développer des programmes de ransomware-as-a-service qui regroupent des méthodes d'attaque éprouvées en playbooks reproductibles et automatisés. Cela a permis à des opérateurs moins expérimentés de mener des campagnes efficaces, un peu comme un commercial junior peut réussir en utilisant un script élaboré à partir des méthodes d'un des meilleurs vendeurs.

Pourquoi les petites organisations sont désormais exposées

L'automatisation, l'apprentissage automatique et l'automatisation robotisée des processus permettent à ces opérateurs de mener de nombreuses attaques simultanément, de gérer les négociations de rançon et de superviser à grande échelle le paiement ou le support à la récupération. Une fois ces fonctions largement automatisées, cibler des entreprises plus petites est également devenu rentable, car ce sont des machines — et non des personnes — qui assurent la majeure partie des démarches et du suivi.

Ce changement rend les attaquants moins sélectifs. Les grandes cibles de type « big game » continuent d'attirer l'attention en raison de l'ampleur du gain potentiel, mais l'activité quotidienne de ces organisations criminelles ressemble de plus en plus à de la prospection commerciale routinière : des systèmes automatisés recherchent en permanence toute organisation susceptible de payer. Les systèmes chargés du ciblage n'ont généralement aucune conscience de la nature réelle de la cible, qu'il s'agisse d'une grande entreprise ou d'une petite association à but non lucratif.

Ce que cela signifie pour les organisations

Étant donné que le ciblage est en grande partie automatisé et indiscriminé, la question la plus pertinente pour la plupart des organisations n'est pas de savoir si elles pourraient être spécifiquement visées, mais dans quelle mesure elles sont préparées à une éventuelle tentative. Des solutions telles que Cyber Crucible, construites sur FortressAI, sont conçues pour aider les organisations à détecter et à stopper les ransomwares et les menaces associées, quelle que soit la taille ou le profil de la cible.

https://player.vimeo.com/video/1047715793?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Qui court le plus grand risque d'une attaque par rançongiciel, et pourquoi ces cibles sont-elles visées ?

Réponse courte : Le risque de rançongiciel dépend souvent de qui les « courtiers d'accès » criminels trouvent le plus facile à pirater, ou sont spécifiquement payés pour pirater, ce qui signifie que les écoles, les hôpitaux et les fournisseurs d'infrastructures dotés de défenses plus faibles ou de données précieuses figurent fréquemment en tête de liste.

Comment les cibles sont choisies dès le départ

Derrière la plupart des incidents de rançongiciel se cache un marché que la plupart des gens ne voient jamais. Un groupe, souvent appelé courtiers d'accès initial, passe son temps à s'introduire dans des réseaux sans plan précis quant à la suite des événements. Une fois qu'ils ont pris pied, ils mettent cet accès en vente, en décrivant exactement ce qu'ils contrôlent, comme des droits administratifs sur des outils de sécurité, la capacité de désactiver les protections antivirus, ou l'accès à une grande partie des appareils d'une organisation. Ils peuvent décrire, par exemple, avoir compromis le parc d'appareils d'un district scolaire ou les outils d'accès à distance d'un prestataire informatique. Les acheteurs, allant des groupes de vol de données aux opérateurs de rançongiciels en passant par des acteurs parrainés par des États, enchérissent alors sur cet accès en fonction de sa valeur et de son exhaustivité apparentes.

Quand les attaques sont commanditées, et non simplement opportunistes

Il existe également un second schéma, plus ciblé. Dans ce cas, un acheteur, tel qu'un groupe de rançongiciels ou un acteur étatique, formule une demande précise : trouver et compromettre un

nombre défini d'organisations répondant à certains critères, comme des hôpitaux d'une taille donnée dans une région donnée, ou des fournisseurs de services publics tels que des stations de traitement des eaux. Les courtiers d'accès traitent alors cela comme une mission commerciale, en recherchant activement des organisations correspondant au profil demandé. Une fois qu'ils réussissent, ils revendent cet accès au demandeur initial, bien que les deux parties n'interagissent généralement jamais directement et ne connaissent pas leurs identités respectives. C'est pourquoi des vagues soudaines d'attaques contre des organisations similaires, comme plusieurs hôpitaux dans une même région, reflètent souvent une commande d'achat coordonnée plutôt qu'une simple coïncidence.

Pourquoi cela compte pour la défense

Parce que le ciblage peut être à la fois opportuniste ou spécifiquement commandité, toute organisation dotée de contrôles de sécurité faibles, de données sensibles ou de services critiques peut devenir une cible, quel que soit sa taille ou son secteur d'activité. Comprendre cette dynamique acheteur-vendeur souligne pourquoi des défenses proactives et fonctionnant en permanence importent bien davantage qu'une réaction après qu'une intrusion a déjà été vendue au plus offrant.

https://player.vimeo.com/video/1047715835?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Qui mène réellement les attaques par rançongiciel et comment opèrent-elles ?

Réponse courte : Les attaques par rançongiciel sont menées par un réseau organisé de manière lâche composé de développeurs, de revendeurs et d'opérateurs qui fonctionnent un peu comme une chaîne d'approvisionnement commerciale, et les plus efficaces d'entre eux traitent l'extorsion comme un métier professionnel plutôt que comme une rancune personnelle.

Le rançongiciel en tant que chaîne d'approvisionnement organisée

Un rançongiciel est rarement l'œuvre d'un seul pirate agissant seul. Il fonctionne plutôt comme une industrie distribuée composée de développeurs de logiciels malveillants qui conçoivent les outils, de revendeurs ou d'affiliés qui distribuent l'accès à ces logiciels malveillants, et d'opérateurs qui mènent les attaques réelles contre les victimes. Chaque groupe joue un rôle distinct, un peu comme un éditeur de logiciels légitime pourrait s'appuyer sur des fabricants, des distributeurs et des équipes commerciales. Cette structure en couches contribue à la résilience du rançongiciel : perturber un maillon de la chaîne n'arrête pas nécessairement l'ensemble de l'opération.

Les professionnels contre les attaquants émotifs

Tous les attaquants ne réagissent pas de la même manière une fois leurs tentatives bloquées. Cyber Crucible a directement fait l'expérience de ce contraste. Dans un cas, un attaquant lié à l'Europe de l'Est a appelé après avoir été stoppé, traitant la rencontre comme un défi technique à résoudre plutôt que comme une insulte personnelle. Cette personne a même mentionné des détails internes sur le logiciel pour prouver qu'elle avait effectué une rétro-ingénierie du produit, puis a continué à reprendre contact périodiquement par la suite, discutant de ses opérations presque comme le ferait un pair.

En revanche, un autre attaquant lié au Bangladesh a réagi avec colère et hostilité après avoir été contrecarré, recourant aux insultes plutôt qu'à la résolution de problèmes. Ce contact n'a pas

poursuivi les échanges dans la durée.

Pourquoi cela compte pour la défense

Ces expériences suggèrent que les acteurs malveillants les plus « efficaces » et persistants ont tendance à être ceux qui abordent le rançongiciel comme un défi commercial — méthodiques, patients et concentrés sur la recherche de contournements. Comprendre les attaquants comme des adversaires professionnels, plutôt que comme de simples criminels chaotiques, contribue à orienter la conception de technologies défensives telles que FortressAI de Cyber Crucible : anticiper les tentatives calculées de contournement des protections, et pas seulement les attaques isolées ou motivées par l'émotion.

https://player.vimeo.com/video/1047715866?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Quel est le client idéal pour la protection contre les rançongiciels de Cyber Crucible ?

Réponse courte : Cyber Crucible convient le mieux aux personnes qui raisonnent en termes d'impact commercial, et pas seulement de fonctionnalités techniques. Cela inclut les responsables informatiques aux ressources limitées ainsi que les dirigeants qui comprennent ce qu'une interruption, même courte, pourrait coûter à l'entreprise.

Pourquoi la logique commerciale compte plus que l'intitulé du poste

Il n'existe pas un intitulé de poste unique qui définisse le client idéal de Cyber Crucible. Ce qui compte, c'est de savoir si la personne saisit les conséquences réelles d'un incident de rançongiciel ou de vol de données : perte de revenus, perturbation des opérations, et le type de dommage financier qui peut persister pendant des mois, voire des années. Une personne dans cet état d'esprit n'a pas besoin d'être convaincue que la prévention automatisée en vaut la peine ; elle comprend déjà que l'évitement des interruptions est directement lié à la préservation des bénéfices et à la continuité de l'activité.

Cela diffère d'une conversation commerciale purement technique, où la valeur d'un produit se perd dans un jargon que seuls les spécialistes peuvent suivre. L'approche de Cyber Crucible, propulsée par FortressAI, a été conçue autour d'un résultat simple et concret pour les clients avant tout, la technologie sous-jacente ayant été construite pour soutenir ce résultat. C'est pourquoi les échanges les plus clairs ont généralement lieu avec des personnes qui se préoccupent de ce que signifie une défaillance de sécurité pour l'entreprise, et pas seulement du fonctionnement interne du logiciel.

Exemples d'interlocuteurs pertinents

Un directeur informatique gérant un personnel et un budget limités, personnellement responsable de la disponibilité et de la fiabilité des systèmes, perçoit souvent rapidement la valeur de la

solution, car les interruptions affectent directement sa charge de travail quotidienne et sa performance. À l'autre extrémité, un PDG ou un directeur financier peut insister pour obtenir une protection automatisée même lorsque l'équipe de sécurité se dit satisfaite des mesures existantes, tout simplement parce qu'il sait qu'une courte interruption, parfois d'à peine une heure, peut engendrer un dommage financier dont la récupération prend bien plus d'un an.

Le fil conducteur commun

Que la conversation débute avec un responsable informatique axé sur les opérations ou avec un dirigeant à la sensibilité financière, le meilleur profil pour Cyber Crucible reste toute personne qui évalue la cybersécurité sous l'angle de la continuité des activités et du risque financier, plutôt que sous celui des seuls détails techniques.

https://player.vimeo.com/video/1046877762?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Pourquoi les attaques par rançongiciel deviennent-elles plus fréquentes chaque année ?

Réponse courte : Les attaques par rançongiciel augmentent parce que les groupes cybercriminels sont passés d'acteurs désorganisés et opportunistes à des opérations disciplinées qui utilisent l'automatisation pour attaquer efficacement de nombreuses victimes et obtenir rapidement un paiement.

De startups chaotiques à des opérations organisées

Lorsque le rançongiciel est devenu une menace répandue, de nombreux attaquants manquaient d'expérience. Une vague de personnes nouvellement au chômage pendant la période pandémique a tenté sa chance dans la cybercriminalité, souvent avec des résultats inégaux. Comme dans toute industrie émergente, seuls les opérateurs les plus organisés et les plus compétents ont survécu à cette première période de tri. Avec le temps, ces groupes ont commencé à fonctionner moins comme des opportunistes dispersés et davantage comme des entreprises structurées axées sur des revenus constants.

D'ici 2024, cette maturité s'est traduite par une forte dépendance à l'automatisation. Les opérations de rançongiciel établies utilisent désormais des outils automatisés pour intégrer des participants moins expérimentés dans leurs attaques tout en maintenant des processus efficaces et reproductibles. Cela leur a permis d'étendre leurs activités bien au-delà de ce qu'une petite équipe de pirates informatiques qualifiés pourrait accomplir manuellement.

Calibrer l'attaque pour un gain maximal

Un élément clé de cette évolution consiste à apprendre à dimensionner correctement une attaque. Si une intrusion est trop mineure, une équipe informatique bien préparée peut simplement restaurer les systèmes et éviter de payer quoi que ce soit. Si une attaque est trop étendue, anéantissant toute l'infrastructure de l'entreprise, il se peut qu'il ne reste aucune activité viable pour effectuer un paiement de rançon. Les groupes de rançongiciel modernes visent un juste milieu : suffisamment de perturbation pour pousser une entreprise à payer rapidement, sans

causer des dommages tels que la reprise ou la négociation deviennent sans objet.

Pourquoi l'automatisation entraîne cette augmentation

Une fois qu'un processus d'attaque peut être automatisé, les cybercriminels ne se contentent plus de viser une seule victime à la fois. À l'aide d'outils qui s'apparentent à l'intelligence artificielle, à l'apprentissage automatique et à l'automatisation robotisée des processus, ils peuvent cibler simultanément des dizaines, voire des centaines d'organisations. De nombreuses victimes choisissent de ne pas divulguer publiquement les incidents, ce qui permet aux attaquants d'achever un cycle d'extorsion et de passer à de nouvelles cibles. Ce modèle économique évolutif et reproductible — plutôt qu'une quelconque nouvelle technologie isolée — est la principale raison pour laquelle les attaques par rançongiciel continuent d'augmenter.

https://player.vimeo.com/video/1043463561?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Pourquoi Cyber Crucible utilise-t-il l'IA plutôt qu'une équipe SOC humaine pour arrêter les rançongiciels ?

Réponse courte : Cyber Crucible a été conçu comme un système entièrement automatisé dès le premier jour, car les attaques par rançongiciel se déroulent bien plus rapidement que ce qu'une équipe de sécurité humaine peut gérer, et l'intelligence artificielle est le seul moyen pratique de modéliser le comportement d'une attaque et d'agir en conséquence en temps réel.

Le problème lié à la dépendance aux temps de réaction humains

Lorsque Cyber Crucible a été développé pour la première fois, vers 2019, les rançongiciels dépassaient déjà la capacité des équipes des opérations de sécurité à réagir. Même les premières souches de rançongiciels pouvaient verrouiller l'ensemble des systèmes d'une organisation en quelques minutes. Cela ne laissait aucune fenêtre réaliste permettant à une personne de repérer les signes d'alerte, d'évaluer la situation et d'intervenir avant que des dommages importants ne surviennent. Depuis, les attaques n'ont fait qu'accélérer : certains rapports suggèrent que le réseau d'une entreprise de taille moyenne peut être entièrement compromis en aussi peu que 90 secondes. À cette vitesse, s'attendre à ce qu'un analyste humain détecte et arrête une attaque en cours n'est simplement pas envisageable, quelle que soit la compétence ou l'effectif de l'équipe.

Pourquoi la modélisation comportementale nécessite l'IA

Arrêter une attaque aussi rapide exige plus que des alertes rapides : cela nécessite un logiciel capable de reconnaître des schémas de comportement malveillant et de prendre une décision de confinement instantanément, sans attendre qu'une personne interprète les données. Construire manuellement ce type de modélisation comportementale détaillée, couvrant les nombreuses façons dont une attaque peut se dérouler, prendrait bien plus de temps que ce dont dispose

n'importe quel défenseur. L'intelligence artificielle est devenue l'outil nécessaire pour construire ces modèles comportementaux avec suffisamment d'efficacité pour qu'ils puissent être intégrés directement dans un logiciel de sécurité, permettant ainsi de prendre des décisions au moment même où une attaque débute plutôt qu'après coup.

L'IA, une nécessité pratique et non une tendance

L'évolution vers une défense pilotée par l'IA n'était pas une question de suivi d'une tendance sectorielle : c'était une réponse pratique à un problème de temporalité que la surveillance humaine ne pouvait pas résoudre. L'approche de Cyber Crucible reflète l'idée d'adapter le bon outil à la bonne tâche : lorsque les attaques se compriment en quelques secondes, la défense doit opérer à la même échelle de temps, ce qui implique une prise de décision automatisée fondée sur l'IA plutôt qu'un examen manuel.

https://player.vimeo.com/video/1046871333?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Pourquoi les équipes de sécurité reçoivent-elles des milliers d'alertes par jour, et comment peuvent-elles y faire face ?

Réponse courte : La surcharge d'alertes n'est pas apparue du jour au lendemain — elle s'est accumulée progressivement à mesure que les attaquants devenaient plus automatisés et plus évasifs, transformant des signaux d'alerte autrefois clairs en indices faibles et ambigus nécessitant une expertise approfondie pour être interprétés. Cyber Crucible a été conçu pour briser ce cycle en gérant automatiquement la détection et la réponse, plutôt qu'en demandant aux équipes humaines de trier d'innombrables signaux à faible fiabilité.

Comment la fatigue liée aux alertes est devenue la norme

Les systèmes d'alerte en sécurité ne se sont pas dégradés parce que les éditeurs ont décidé de reporter la charge sur leurs clients. Cela s'est produit lentement, à mesure que les attaquants perfectionnaient leurs techniques pour muter et s'automatiser plus vite que les outils défensifs ne pouvaient qualifier un événement de malveillant avec certitude. Ce qui constituait autrefois un indicateur clair de compromission est devenu un indice ténu, noyé parmi d'innombrables autres indices tout aussi ténus. Les trier correctement demande un temps considérable à des analystes chevronnés, et souvent, ce qui semble suspect n'est rien de plus qu'un pilote d'imprimante défaillant. Pendant ce temps, une seule alerte à faible fiabilité négligée peut être la seule trace visible d'une intrusion active et grave.

Pourquoi davantage d'alertes n'a pas amélioré la sécurité

À mesure que les outils de détection tentaient de suivre le rythme des menaces en constante évolution, ils ont compensé en signalant tout ce qui semblait tant soit peu inhabituel. Cela a créé un flot d'alertes qui, techniquement, remplissait l'exigence d'avertir les clients, mais laissait les

équipes de sécurité dans l'incapacité réaliste d'enquêter sur chacune d'elles. Le résultat naturel est l'un des deux scénarios suivants : les équipes commencent à ignorer les alertes à faible fiabilité — précisément là où les attaquants sophistiqués ont tendance à se dissimuler — ou elles se retrouvent submergées, et le travail critique n'est tout simplement pas accompli, quels que soient les efforts ou les intentions.

Un point de départ différent

Conscient que des correctifs incrémentaux ne résoudraient pas un problème enraciné dans des années de complexité accumulée, Cyber Crucible a abordé la question sous un angle entièrement différent. Plutôt que de générer davantage d'alertes à trier par des humains, notre technologie FortressAI est conçue pour détecter et neutraliser de manière autonome, en temps réel, les menaces liées aux rançongiciels, au vol de données et à l'usurpation d'identité. En s'appuyant sur des approches modernes telles que l'IA générative, Cyber Crucible vise à réduire la dépendance à l'examen manuel des alertes et à corriger le déséquilibre sous-jacent entre l'automatisation des attaquants et la capacité des défenseurs.

https://player.vimeo.com/video/1186492629?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Pourquoi le vol d'identifiants et d'identité est-il plus dangereux que le chiffrement par ransomware ?

Réponse courte : Le chiffrement par ransomware est l'étape visible et finale d'une attaque, mais les dégâts réels surviennent souvent plus tôt, de manière inaperçue, lorsque les attaquants récupèrent automatiquement les mots de passe, les jetons de session, les clés et les portefeuilles de cryptomonnaies. Cyber Crucible se concentre sur la détection et l'arrêt de cette étape précoce et cachée, plutôt que d'attendre le moment où les données sont verrouillées.

Pourquoi les outils de sécurité passent souvent à côté de la menace la plus importante

De nombreux produits de sécurité sont conçus pour réagir au chiffrement, car c'est la partie de l'attaque qu'une entreprise remarque réellement : les systèmes tombent en panne, les fichiers deviennent illisibles et les opérations s'arrêtent. Cette perturbation visible attire naturellement le plus d'attention et d'investissements. Cependant, le chiffrement est généralement la dernière action entreprise par un attaquant, et non la première. Au moment où une entreprise constate les effets d'un ransomware, l'attaquant a généralement déjà achevé la partie la plus lourde de conséquences de l'intrusion : la collecte discrète de données liées à l'identité, telles que les identifiants, les jetons d'authentification, les clés de chiffrement et l'accès aux portefeuilles numériques. Cette phase précoce ne provoque aucune perturbation visible, ce qui explique qu'elle soit souvent sous-estimée, alors même qu'elle offre aux attaquants un accès durable et répétable au réseau.

La première étape silencieuse d'une attaque

Les attaques modernes sont largement automatisées, et la phase de vol d'identité peut être menée à bien en quelques secondes seulement à l'échelle de toute une organisation. Comme il n'y a pas d'interruption immédiate de l'activité, cette étape ne bénéficie pas de l'urgence et de la visibilité que crée le chiffrement par ransomware, ce qui la rend facile à négliger. Pourtant, c'est bien cette étape qui donne aux attaquants la possibilité de revenir quand ils le souhaitent et de causer des dommages supplémentaires, y compris de déployer un ransomware par la suite.

Comment Cyber Crucible répond à cette lacune

Cyber Crucible est conçu pour détecter les accès non autorisés aux données d'identité au moment même où ils se produisent, plutôt que d'attendre le début du chiffrement. Étant donné que cette activité se déroule si rapidement et si discrètement, des efforts d'ingénierie considérables ont été consacrés à rendre la détection à la fois rapide et précise, afin d'identifier qui accède aux données d'identité sensibles sans ralentir les opérations commerciales quotidiennes ni l'activité des utilisateurs.

https://player.vimeo.com/video/1141670023?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Pourquoi le rançongiciel est-il devenu si difficile à arrêter et dont il est si difficile de se remettre ?

Réponse courte : Le rançongiciel est passé d'une simple astuce de piratage à une opération criminelle mature, organisée comme une entreprise, qui utilise un chiffrement en couches et des clés disparaissantes pour rendre la récupération quasiment impossible sans payer. Comprendre le fonctionnement réel du chiffrement et de la gestion des clés explique pourquoi les sauvegardes, les saisies des forces de l'ordre et les solutions rapides échouent souvent.

En quoi le rançongiciel diffère d'une violation de données

Une violation de données consiste à voler discrètement des informations pour les revendre plus tard, tandis que les opérateurs de rançongiciels ont un objectif différent : rester à l'intérieur d'un réseau juste assez longtemps pour causer un maximum de perturbations, puis se révéler. Une fois les dégâts causés, se cacher n'a plus d'importance pour eux. Cette opération est de plus en plus automatisée et gérée comme une entreprise, avec traitement des paiements et « service client » de déchiffrement, car les attaquants ont besoin d'un moyen fiable de collecter de l'argent à grande échelle.

L'astuce de chiffrement derrière l'attaque

Le rançongiciel repose généralement sur deux types de chiffrement fonctionnant ensemble. Le chiffrement symétrique rapide (comme l'AES) verrouille les fichiers proprement dits, tandis que le chiffrement asymétrique, plus lent — la même méthode utilisée pour sécuriser le trafic Web — protège la clé symétrique elle-même. Il s'agit d'une technique cryptographique bien établie, empruntée à des systèmes de sécurité légitimes, mais dans le cas du rançongiciel, cela signifie que même si la clé d'un seul fichier venait à être récupérée d'une manière ou d'une autre, les

attaquants ont ajouté une complexité supplémentaire de sorte que le déchiffrement d'un fichier dépend souvent de la génération d'une nouvelle clé pour le suivant, rendant les raccourcis bien plus difficiles qu'il n'y paraît.

Pourquoi les options de récupération s'affaiblissent constamment

Les premiers rançongiciels réutilisaient une clé unique pour de nombreuses victimes, ce qui permettait parfois aux défenseurs d'extraire et de partager un outil de déchiffrement. Les attaquants ont réagi en générant des clés uniques, à usage unique, qui ne sont jamais stockées nulle part de manière récupérable. Cela supprime l'option de qu

https://player.vimeo.com/video/1065143398?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Pourquoi les antivirus traditionnels ne peuvent-ils pas arrêter les attaques de ransomware zero-day et sans fichier ?

Réponse courte : Les outils de sécurité basés sur des signatures s'appuient sur la reconnaissance de schémas d'attaque connus, mais les attaquants modernes testent délibérément leurs outils contre ces mêmes défenses avant de les déployer, et évitent de plus en plus de déposer des fichiers détectables. Cette combinaison de menaces mutées et non reconnues, associée à des techniques opérant uniquement en mémoire, a rendu les méthodes de détection traditionnelles beaucoup moins fiables.

Le problème de la dépendance aux signatures connues

Les attaques zero-day sont, par définition, suffisamment nouvelles ou modifiées pour échapper à ce que les outils de sécurité existants reconnaissent déjà. Les fournisseurs promettent depuis longtemps des améliorations pour détecter ces menaces, mais les attaquants disposent d'un avantage inhérent : ils ont accès aux mêmes produits de sécurité commerciaux que ceux utilisés par les défenseurs. Avant de lancer une campagne, les attaquants testent régulièrement leurs logiciels malveillants contre les outils de détection populaires, les affinant jusqu'à ce qu'ils passent inaperçus. Cela transforme la détection en une cible mouvante constante plutôt qu'en une défense fixe.

Les techniques sans fichier compromettent la liste blanche d'applications

Les attaquants ont également cessé de déposer des exécutables malveillants évidents sur un système. Ils détournent à la place des applications légitimes et fiables, déjà approuvées par les outils de liste blanche d'applications, en exécutant des activités malveillantes via des processus que le logiciel de sécurité considère comme sûrs. Lorsque cette approche sans fichier est combinée à un code qui mute rapidement, les attaques peuvent se conclure dans une fenêtre de temps très courte — parfois en une demi-heure — bien avant qu'une équipe humaine de réponse aux incidents ne puisse réalistement mener une investigation.

Les attaquants effacent eux-mêmes leurs traces

Dans de nombreux cas, comme l'attaque réside en mémoire plutôt que sur le disque, les attaquants effacent les journaux, les preuves, voire les capteurs de sécurité avant de terminer leur opération. Cela ressemble à un cambrioleur désactivant les caméras de sécurité et les alarmes avant de commettre un délit : lorsque quelqu'un cherche des preuves, la visibilité la plus utile a déjà été détruite. Cette combinaison de méthodes d'attaque imprévisibles et de preuves autodestructrices explique pourquoi Cyber Crucible a investi des efforts considérables dans la construction d'une approche automatisée et évolutive — conçue pour capturer les données critiques nécessaires à la prise de décisions précises avant que les attaquants ne puissent effacer leurs traces, plutôt que de dépendre de la reconnaissance des menaces après coup.

https://player.vimeo.com/video/1164197533?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Les pirates utiliseront-ils davantage l'IA dans les attaques par rançongiciel en 2025 ?

Réponse courte : Oui. Les attaquants devraient continuer à élargir leur utilisation de l'intelligence artificielle, en particulier des grands modèles de langage, pour usurper l'identité de personnes de confiance et manipuler les victimes afin qu'elles accordent un accès ou leur confiance.

Pourquoi l'IA est devenue une favorite des pirates

Les résultats de recherche, les fils d'actualités et les conversations quotidiennes sont désormais saturés de références à l'IA, et cet engouement s'est également emparé des cybercriminels. Lorsque la plupart des gens mentionnent l'IA, ils font généralement référence à des grands modèles de langage comme ceux qui alimentent ChatGPT et des outils similaires capables d'imiter de manière convaincante la communication humaine. Les attaquants ont reconnu que cette capacité est extrêmement utile pour l'ingénierie sociale. Plutôt que de s'appuyer sur des e-mails de phishing génériques, ils peuvent générer des messages, des voix ou des conversations qui ressemblent étroitement à un vrai collègue, fournisseur ou figure d'autorité, ce qui rend beaucoup plus facile de gagner la confiance d'une cible avant de frapper.

Attendez-vous à des tactiques d'usurpation d'identité plus raffinées

La tendance à l'approche de 2025 n'est pas que les attaques pilotées par l'IA soient totalement nouvelles, mais qu'elles deviennent plus soignées et professionnelles. De la même manière que les entreprises légitimes déploient des agents de vente pilotés par l'IA et des outils de prospection automatisés, les attaquants affinent leurs propres techniques d'usurpation d'identité basées sur l'IA. Cela signifie des messages plus convaincants imitant des patrons, des collègues ou des partenaires de confiance, tous conçus pour exploiter les relations de travail dont dépendent les gens au quotidien. Le danger est qu'une conversation qui semble personnelle et légitime puisse en réalité provenir d'un système d'IA hautement performant conçu pour manipuler, et non pour aider.

Ce que cela signifie pour la défense

À mesure que ces tactiques d'usurpation d'identité se perfectionnent, les organisations doivent partir du principe que les attaques basées sur la confiance deviendront plus difficiles à repérer par instinct seul. Vérifier les demandes par des canaux indépendants, plutôt que de faire confiance à un message ou à un appel sur la seule apparence, devient de plus en plus important. Étant donné que ces attaques sont conçues pour contourner le jugement humain, disposer de capacités de détection et de réponse automatisées, telles que celles intégrées dans FortressAI de Cyber Crucible, offre une couche de protection supplémentaire lorsque l'ingénierie sociale parvient à déjouer les défenses d'une personne.

https://player.vimeo.com/video/1046827321?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

L'utilisation de Cyber Crucible réduit-elle le budget de sécurité global d'une entreprise ?

Réponse courte : Cyber Crucible n'est pas conçu pour réduire directement votre budget de sécurité ; il libère plutôt le temps et les ressources humaines qui étaient auparavant consacrés à la surveillance manuelle et à la traque des faux positifs, afin que vous puissiez réorienter cette capacité vers les lacunes de sécurité que vous ne pouviez auparavant pas vous permettre de traiter.

Pourquoi l'automatisation ne signifie pas automatiquement des économies

Il est tentant de supposer que remplacer les processus de sécurité manuels par un outil automatisé comme Cyber Crucible réduirait immédiatement les coûts. Dans la pratique, ce n'est généralement pas ainsi que les choses se déroulent. De nombreux programmes de sécurité reposent sur un assemblage d'outils qui nécessitent un réglage constant, une supervision et un examen manuel des alertes. Lorsque vous introduisez une automatisation qui réduit cette charge pratique, la valeur ajoutée ne réside pas principalement dans une facture plus basse, mais dans le temps et l'attention récupérés par votre équipe. Cette capacité récupérée a tendance à être réinvestie dans d'autres priorités de sécurité plutôt que d'être comptabilisée comme une économie pure.

Où la véritable valeur se manifeste

La plupart des responsables informatiques et de la sécurité savent déjà que leur liste de tâches dépasse le personnel et les outils dont ils disposent. Les effectifs limités et les contraintes techniques font que de nombreux risques connus restent tout simplement non traités. En réduisant l'effort manuel consacré au tri des faux positifs et à la surveillance des systèmes de détection, Cyber Crucible offre aux équipes la marge de manœuvre nécessaire pour enfin s'attaquer à ces problèmes négligés. En ce sens, l'avantage réside dans la flexibilité et le contrôle budgétaires, et non nécessairement dans un budget réduit. Les responsables peuvent choisir de réduire les dépenses, de les réaffecter ou d'étendre la couverture à des domaines auparavant hors de portée en raison de contraintes de ressources.

Ce que Cyber Crucible peut et ne peut pas promettre

Cyber Crucible ne peut pas résoudre toutes les contraintes budgétaires auxquelles une organisation est confrontée. Ce qu'il peut faire, c'est donner aux responsables de la sécurité davantage de maîtrise sur la manière dont leurs dépenses se traduisent en protection réelle. En remplaçant la surveillance manuelle et exigeante en main-d'œuvre par une défense automatisée, les équipes acquièrent la capacité d'orienter leur budget existant vers le renforcement de l'efficacité globale du programme de sécurité qu'elles ont construit, plutôt que de le dépenser à maintenir des outils qui exigent une attention constante.

https://player.vimeo.com/video/1043470826?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية