PENTERA

(Anciennement Pcysys)

Pentera RansomwareReady™

Émulez aujourd'hui. Être sécurisé pour demain.

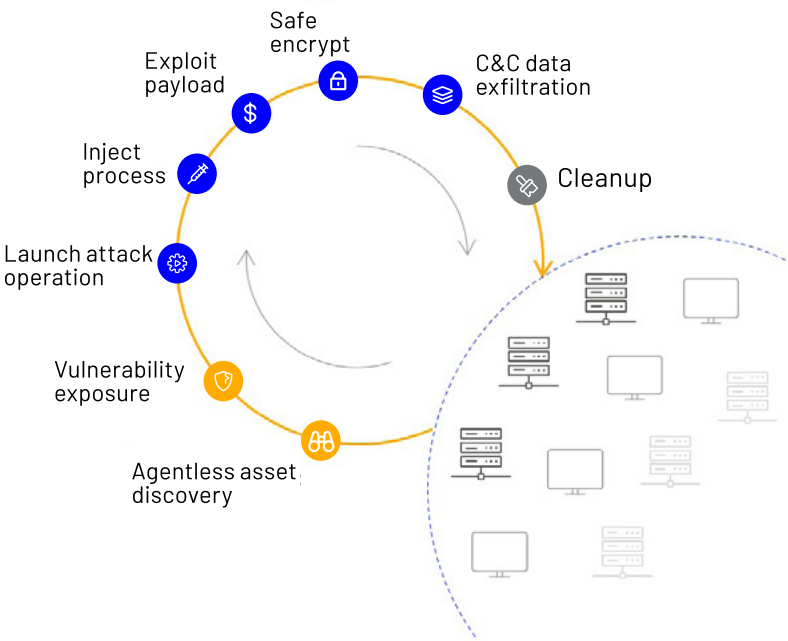
Les attaques de type Ransomware ont rapidement augmenté en fréquence et en gravité. Considéré à l'origine comme une simple nuisance, le Ransomware est maintenant adopté par des pirates sophistiqués, pour des attaques complexes et multi-tenant impliquant le chiffrement et la prise en otages de données. Ces acteurs ont élargi leur champ d'action, passant de la diffusion à grande échelle de ce malware (logiciel malveillant) au ciblage d'organisations et d'industries spécifiques, voire parfois de villes entières. Aujourd'hui, le coût total des attaques par Ransomware se chiffre en millions de dollars.

C'est pourquoi Pentera, notre plateforme logicielle de Cyber Validation Automatique, inclut à présent le premier cadre d'émulation active de Ransomware, appliquant des tactiques et techniques réelles à la structure de votre organisation, en toute sécurité. Ce cadre vous permet de valider à tout moment la capacité de votre organisation à contrer une attaque par Ransomware. Nous ne cherchons pas à détecter le Ransomware, nous soumettons votre entreprise à une simulation de crise.

Validez votre Cyber-Résilience.

RansomwareReady™ applique les versions inoffensives des souches de Ransomware les plus destructrices trouvées dans la nature. La plateforme Pentera émule une attaque complète par Ransomware, afin de détecter les vulnérabilités les plus exploitables et les mouvements latéraux que les Cybercriminels pourraient emprunter pour cibler vos infrastructures critiques et nuire aux opérations.

Une fois l'énumération de vos devices effectuée grâce à un déploiement Agentless et les vulnérabilités exploitables détectées, Pentera explore votre réseau, de l'exploitation initiale à l'exécution exclusive de payloads, en passant par le chiffrement et l'exfiltration des données, sous format MITRE ATT&CK™.



Agir avant qu'il ne soit trop tard.

Dans quelle mesure les équipes de sécurité sont-elles convaincues que leurs contrôles de défense fonctionnent réellement comme prévu ? La prévention et la détection ne suffisent pas.. Pentera expose clairement l'ampleur et la profondeur d'une attaque de type Ransomware à travers votre réseau et son impact potentiel sur votre entreprise. Si les équipes informatiques ne testent pas en permanence leurs contrôles de sécurité, elles savent que quelqu'un d'autre le fera pour elles.

Connaître l'impact d'un Ransomware

À mesure que votre empreinte numérique s'accroît, les vulnérabilités et les faiblesses en matière de sécurité augmentent également. Dans le cas du Ransomware, les équipes de sécurité ne peuvent pas se permettre de négliger des failles de sécurité, ni d'opérer des simulations uniquement sur un sous-ensemble de leur réseau. Un simple résultat de type réussite/échec ne suffit pas à prouver la protection de votre système et crée un faux sentiment de sécurité. Si Pentera découvre sur votre réseau des assets critiques et vulnérables, nous déclenchons alors une attaque complète par Ransomware. Pentera applique une méthode de priorisation concluante qui accélère les étapes de remédiation en fonction du risque réel pour l'entreprise. Cette approche réduit considérablement tout risque d'une future attaque par Ransomware.

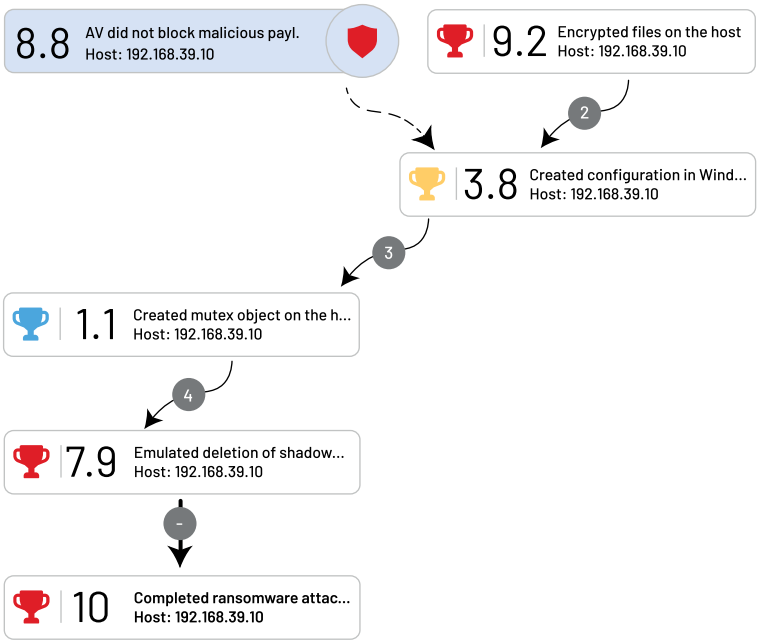
Principaux avantages

- Réduire l'impact de la menace et du Ransomware
- Renforcer le réseau et l'état opérationnel
- Accélérer le cycle validation-remédiation
- Garantir en continu l'efficacité de votre système de sécurité

Pourquoi Pentera ?

Avec Pentera, aucune compétence particulière n'est requise. Quelle que soit sa taille ou son expertise, votre équipe de sécurité sera plus à même de connaître l'état opérationnel de ses contrôles et sa capacité à faire face à une attaque par Ransomware. Passez plus de temps à renforcer votre réseau et moins de temps à corriger des vulnérabilités non pertinentes. L'interface utilisateur intuitive de la plateforme Pentera a été conçue pour accroître l'efficacité de votre équipe de sécurité, en automatisant en permanence le processus de validation dans un réseau hybride et distribué.

Pentera permet à tout membre d'une équipe informatique de comprendre rapidement la cause d'une attaque et d'appliquer immédiatement la meilleure solution à sa remédiation.



Agir

Les pirates passent de nombreuses années à perfectionner leurs attaques par ransomware. Malgré cela, Pentera peut vous aider. Notre plateforme vous permet d'assurer l'état opérationnel de votre réseau, et nous lutterons à vos côtés pour garantir votre protection. Prêt à l'emploi en quelques minutes, Pentera expose les assets critiques par l'émulation d'attaques exhaustives de ransomware et le ciblage de vulnérabilités profondes, afin de rendre votre organisation RansomwareReady™.

En savoir plus sur www.pentera.io

Contactez-nous pour une évaluation, à notre charge, de votre posture de cybersécurité contre les Ransomware.