PENTERA
(früher Pcysys)

Pentera RansomwareReady™

Heute validieren. Morgen bereit sein.

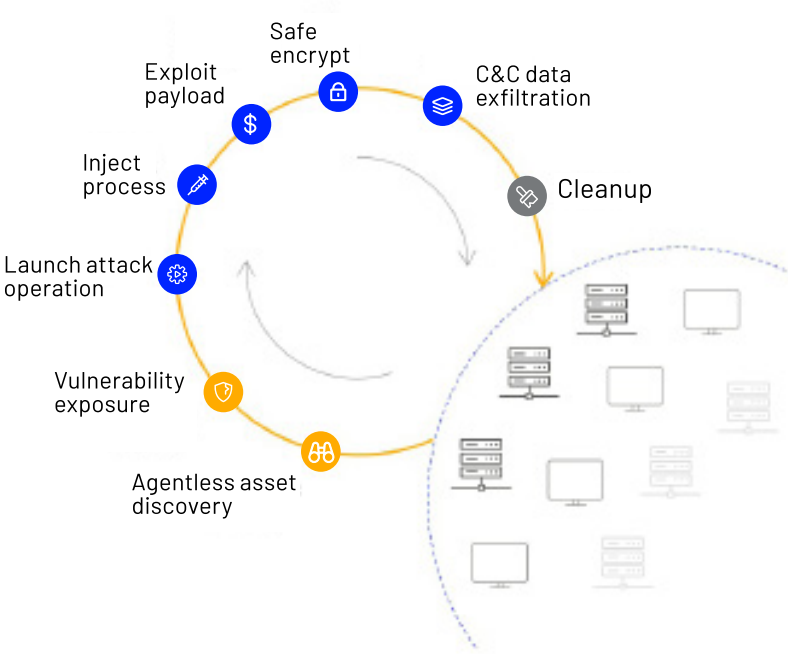
Ransomware-Angriffe haben in ihrer Häufigkeit und Schwere rapide zugenommen. Was anfangs als lästiges Übel angesehen wurde, wird nun von raffinierten Angreifern in komplexen, mehrstufigen Angriffen genutzt, um die Datenverschlüsselung mit der Gefahr der Datenpreisgabe zu kombinieren. Diese Akteure haben ihren Aktionsradius vergrößert - von einer weit verbreiteten Malware-Bedrohung bis hin zu gezielten Angriffen auf bestimmte Organisationen und Branchen - einschließlich ganzer Städte. Heute können die Gesamtkosten von Ransomware-Angriffen in die Millionen gehen.

Aus diesem Grund hat Pentera, die automatisierte Sicherheitsvalidierungsplattform, das erste aktive Ransomware-Emulations-Framework hinzugefügt, das echte und sichere Ransomware-Taktiken und -Techniken auf das Framework Ihrer Organisation anwendet. Dieses Framework ermöglicht es Ihnen, die Bereitschaft Ihrer Organisation gegen einen Ransomware-Angriff zu jedem beliebigen Zeitpunkt zu überprüfen. Wir versuchen nicht, Ransomware aufzuspüren - wir testen Ihre Organisation auf ihre Widerstandsfähigkeit.

Das einzig Wahre. Bestätigt.

RansomwareReady™ wendet sichere Versionen der destruktivsten Ransomware-Stämme an, die in freier Wildbahn gefunden wurden. Die Pentera-Plattform emuliert einen kompletten Ransomware-Angriff, um die wahrscheinlichsten Schwachstellen und seitlichen Pfade zu erkennen, die Ransomware einschlagen wird, um kritische Anlagen anzugreifen und den Betrieb zu stören.

Sobald die agentenlose Asset-Erkennung und die Aufdeckung von Schwachstellen abgeschlossen ist, bewegt sich Pentera durch Ihr Netzwerk. Von der anfänglichen Ausnutzung über die Ausführung von proprietären Nutzdaten bis hin zur Verschlüsselung und Datenexfiltration, die vollständig auf das MITRE ATT&CK-Framework abgestimmt sind.



Handeln vor dem Kompromiss

Prävention und Erkennung allein reichen nicht aus. Wie zuversichtlich sind Sicherheitsteams, dass ihre Verteidigung Kontrollen wirklich wie vorgesehen funktionieren? Mit der automatisierten Sicherheitsvalidierung von Pentera können Sicherheitsteams ihren Fokus von der Reaktion auf aktive bösartige Kampagnen auf die Orchestrierung von Angriffsoperationen und Stresstests ihrer Sicherheitskontrollen verlagern. Pentera zeigt klar auf, wie weit und tief sich ein Ransomware-Angriff im Netzwerk ausbreitet und welche Auswirkungen dies auf den Betrieb haben kann. IT- und Sicherheitsteams wissen, dass, wenn sie ihre Sicherheitskontrollen nicht kontinuierlich testen, dies jemand anderes für sie tun wird.

Das wahre Risiko eines Ransomware-Angriffs kennen

Mit dem Wachstum Ihres digitalen Fußabdrucks wachsen auch die Schwachstellen und Sicherheitslücken. Im Falle von Ransomware können es sich die Sicherheitsteams nicht leisten, Sicherheitslücken zu übersehen oder nur eine Teilmenge ihres Netzwerks zu simulieren. Eine einfache Pass/Fail-Ausgabe impliziert keine Bereitschaft und schafft ein falsches Gefühl von Sicherheit. Sobald Pentera kritische Assets im Netzwerk entdeckt, die für einen Angriff anfällig sind, wird ein vollständiger Ransomware-Angriff ausgelöst. Pentera bietet eine geführte Schritt-für-Schritt-Sanierung, welche auf Grundlage des tatsächlichen Risikos für das Unternehmen priorisiert wird. Dadurch wird das Risiko eines zukünftigen Ransomware-Angriffs drastisch reduziert.

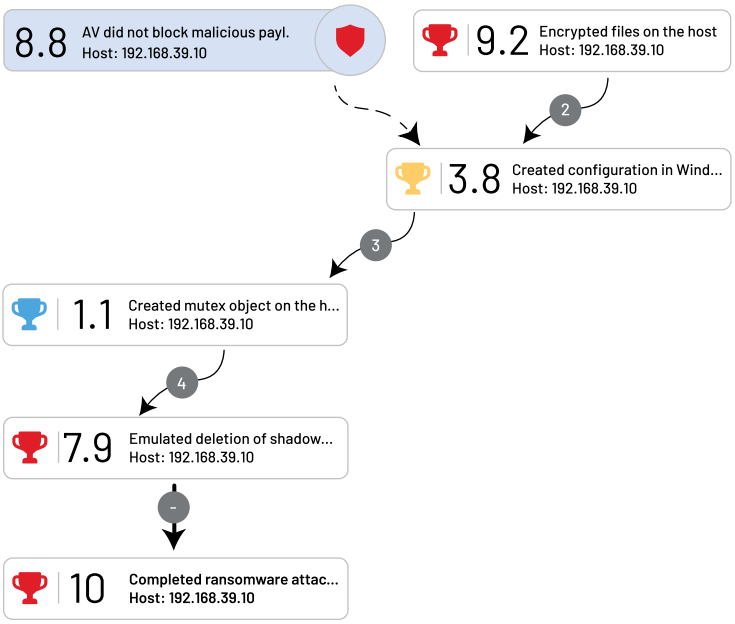
Vorteile

- Geringere Auswirkungen von Bedrohungen und Ransomware
- Gehärtetes Netzwerk und Sicherheitsbereitschaft
- Beschleunigter Validierungs- und Korrekturzyklus
- Garantierte kontinuierliche Überprüfung der Wirksamkeit Ihrer Sicherheits Infrastrukut

Warum Pentera

Mit Pentera sind keine besonderen Kenntnisse erforderlich. Sicherheitsteams jeder Größe und jedes Reifegrades können sich einen Überblick über die Wirksamkeit ihrer Sicherheitskontrollen und die Bereitschaft des Unternehmens für einen Ransomware-Angriff verschaffen. Verbringen Sie mehr Zeit mit der Unterstützung des Unternehmens und weniger Zeit mit dem Patchen irrelevanter Schwachstellen. Die intuitive Benutzeroberfläche der Pentera-Plattform wurde entwickelt, um die Effizienz des Sicherheitsteams zu erhöhen, indem der Prozess der Sicherheitsvalidierung über das hybride und verteilte Netzwerk des Unternehmens kontinuierlich automatisiert wird.

Pentera befähigt jedes Mitglied des IT-Teams, die Ursachen schnell zu verstehen und sofort den optimalen Weg zur Behebung zu finden.



Maßnahmen ergreifen

Angreifer haben viele Jahre damit verbracht, die Ransomware-Angriffsoperation zu perfektionieren. Trotzdem kann Pentera helfen. Nutzen Sie die Pentera-Plattform, um Ihre Bereitschaft zu gewährleisten, und lassen Sie uns gemeinsam aufhören, eine Niederlage zu akzeptieren. Pentera ist innerhalb von Minuten einsatzbereit, legt kritische Anlagen offen, emuliert komplette Ransomware-Angriffe und deckt die wichtigsten Schwachstellen auf, um Ihr Unternehmen RansomwareReady™ zu machen.