Hat Cyber Crucible Fehlalarme? Wie hoch ist die Fehlalarmquote?

Cyber Crucible strebt eine Produktumgebung mit 0 Fehlalarmen an. Dennoch kommt es gelegentlich zu Fehlalarmen. Lassen Sie uns besprechen, woher diese kommen.

Derzeit liegt die Fehlalarmquote bei etwa 1 Reaktion pro Monat pro 1800 Bereitstellungen/Agenten, mit vollständiger Nachvollziehbarkeit, warum diese Reaktionen auftreten.

Beschädigtes Programm mit schnellen Dateioperationen

Ob absichtlich oder durch fehlerhafte Programmierung – manchmal beschädigen sich Programme selbst oder werden während der Ausführung durch andere Programme beschädigt. Wir sehen dies häufig bei neuen Funktionen in großen Programmpaketen wie Microsoft Office oder proprietärer, individuell entwickelter Software.

Dabei wird der Speicher des Programms beschädigt, was den Umfang der Überprüfung des Programms erhöht. Folgt darauf ein erpressungsähnliches Verhalten beim Dateizugriff, ist Cyber Crucible gezwungen, das Programm zu beenden. Wir werden immer besser darin, bekannte Fehler zu identifizieren, sodass Sie Ihr Programm zumindest bis zum Absturz ausführen können (manche starten automatisch neu, manche nicht).

In einer Welt, in der Angreifer nicht das Dateisystem nutzen, sondern stattdessen den Speicher laufender Programme kapern, müssen wir vorsichtshalber im Zweifel eingreifen.

Cyber Crucible verfügt nun über die Möglichkeit, eine Berechtigung zu erstellen: Wenn Programm A mit Argumenten Argumente A eine Beschädigung in Programm B mit Argumenten Argumente B verursacht, können wir eine temporäre Ausnahme erstellen für:

(Programm A + Argumente A) öffnet (Programm B + Argumente B)

Auf diese Weise wird kein zusätzliches Risiko angenommen, dass ein Hacker beteiligt ist, es sei denn, dieser verwendet zufällig genau dieselben Argumente.

Ein hervorragendes Beispiel dafür war, als Microsoft erstmals das Öffnen von Office-Dokumenten aus ihrer Desktop-Chat-Software einführte. Dies beschädigte das Office-Programm… jedes… einzelne… Mal…. Anschließend begann das Office-Programm in etwa 25 % der Fälle, alle Dokumente auf dem Rechner zu scannen. Das… erforderte eine Ausnahme.

Wenn Sie einen Absturz erleben, nutzen Sie die Support-Schaltfläche, und wir helfen Ihnen dabei, eine Ausnahme zu erstellen, bis der Anbieter das Problem behebt.

Sicherheitsprogramme

Cyber Crucible funktioniert sehr gut im Zusammenspiel mit Sicherheitsprogrammen. Entgegen der Annahme der meisten neuen Kunden nutzen fortschrittlichere Sicherheitstools tendenziell fortschrittlichere Systeminteraktionen als Antivirenprogramme, die ältere Technologien verwenden. Tatsächlich führen einige kostenlose oder kostengünstige Sicherheitstools eine Vielzahl unsicherer PowerShell-Skripte als zentralen Bestandteil ihres Schutzes aus, anstatt tatsächliche Programme.

Als ein hochgradig widerstandsfähiges, kernelbasiertes Sicherheitstool wird Cyber Crucible am besten als „tiefer“ oder „näher“ an der Hardware angesiedelt betrachtet als die meisten anderen Tools. Cyber Crucible identifiziert automatisch andere Sicherheitstools und fügt sie den Verhaltensmodellen hinzu. Solange die Sicherheitstools keine Anzeichen einer Kompromittierung zeigen, dürfen sie normal weiterarbeiten.

Gelegentlich verursacht ein Sicherheitstool Systeminstabilität, wenn dessen Versuche, die Cyber Crucible-Software abzuschalten oder zu beeinträchtigen, fehlschlagen. In solchen Fällen ist es am besten, Cyber Crucible im jeweils anderen Sicherheitstool auf die Whitelist zu setzen, um zu verhindern, dass dieses versucht (und scheitert), Cyber Crucible zu deaktivieren oder zu beeinträchtigen.

Zögern Sie nicht, über das Webportal ein Support-Ticket bei Cyber Crucible zu eröffnen, um die Angelegenheit zu besprechen.

Administrations- oder Backup-Tools

Unter bestimmten Umständen muss ein maßgeschneidertes Verhalten für ein Administrations- oder Backup-Tool erstellt werden, während das Cyber Crucible-Team ein verbessertes Verhaltensmodell entwickelt. In diesem Fall unterstützt das Cyber Crucible-Team bei der Erstellung einer Ausnahme im Verhaltensmodell, die das Programm zusammen mit den Argumenten für ein äußerst kleines

Zeitfenster eines möglichen Angriffs herausfiltert.

Revision #1
Created 2026-07-24 04:40:19 UTC by Dennis Underwood
Updated 2026-07-24 04:40:19 UTC by Dennis Underwood