Handelt es sich hierbei um ein Überwachungstool wie meine anderen Sicherheits-Dashboards?

Die Antwort lautet: Es kommt darauf an, wie Sie und Ihr Unternehmen das Tool nutzen möchten, aber wahrscheinlich „nein“.

Es ist wichtig, die Produktdesign-Strategien von Cyber Crucible zu beachten:

1. Der Schutz sollte hochgradig automatisiert sein und weder ständige Pflege und Zuwendung (Alarmbeachtung) noch Feinjustierung (Konfiguration) durch die Benutzer erfordern.
2. Für ressourcenstärkere Sicherheitsteams sollte die wertvolle Telemetrie für fortgeschrittene Bedrohungsjagd-Aktivitäten oder zur Unterstützung von Forensik- und Incident-Response-Aktivitäten verfügbar sein.
3. Maßnahme Nr. 2 oben sollte den bestehenden Schutz gemäß Maßnahme Nr. 1 in keiner Weise beeinträchtigen.

Die häufigste Rückmeldung, die wir von der IT-Leitung erhalten, ist, dass ihre Mitarbeiter nicht wussten, dass Cyber Crucible sie bereits seit Wochen schützt.

Wir haben viele Benutzer, die das Tool auf drei Arten nutzen:

Einrichten und Vergessen (Wie Ihre Rauchmelder)

Vielen Organisationen fehlen die Ressourcen, um Threat Hunter die Telemetriedaten von Cyber Crucible (oder anderen Tools) durchforsten zu lassen, aber sie möchten das Risiko von Datenerpressung „von ihrem Teller haben“. Das ist völlig in Ordnung, und genau dafür ist Cyber Crucibles Data Extortion Prevention konzipiert.

Diesen Benutzern fehlen die Ressourcen, um Zeit mit der Betrachtung der Datenfeeds zu Process Injection, Credential Protection und Process Creation zu verbringen.

Daher stellen wir fest, dass sie sich, sofern sie nicht auf eine seltene automatisierte Reaktion von Cyber Crucible reagieren oder eine Bestandsverwaltung durchführen, etwa wenn auf einem neuen Rechner Cyber Crucible bereitgestellt werden muss...

...einfach nicht im Cyber Crucible Webportal anmelden und die Automatisierung ihre Arbeit machen lassen.

Das ist völlig in Ordnung!

Fortgeschrittene Bedrohungsjagd + automatisierter Schutz

Die Funktionen Process Injection, Überwachung der Anmeldedatennutzung und Process Creation liefern einen umfangreichen Datensatz, der über verhaltensbasierte Analysen auf Kernel-Ebene erfasst wird, um Bedrohungsjagd durchzuführen.

Der automatisierte Schutz greift, sobald Datendiebstahl, Diebstahl von Anmeldedaten (Token, Passwort) oder Ransomware-Verschlüsselung beginnt. Für alles andere ist dies eine hervorragende Ressource.

Der häufigste Befund bisher sind nicht verwaltete (zumindest von den aktuellen IT-Administratoren) Remote-Management-Tools, die von Benutzern installiert wurden. Ja, dies führt manchmal zu einem automatisierten Erpressungsschutz (d. h., das nicht verwaltete RMM wird von einem böswilligen Akteur genutzt), aber es ist immer besser, im Voraus mehr über Ihre Umgebung zu wissen, unabhängig davon!

Hier ist ein kurzes Video zu einer Angriffsart, die wir bei Angreifern in mehreren Kundenumgebungen beobachtet haben und die erfolgreich zur Umgehung der EDR-Lösungen der Kunden eingesetzt wurde (wir nennen ungern Namen ... es waren 3 Produkte in vier Unternehmen).

rr-com-dll.mp4

Forensische Analyse und Behebung nach einem Vorfall

Es gibt mehrere Anwendungsfälle für Cyber Crucible-Daten.

Der erste besteht darin, dass eine Sicherheits- oder IT-Fachkraft im Unternehmen die Grundursache für die Beendigung eines Programms untersuchen kann. Bei einigen Kunden, die unsere Software typischerweise installieren und sich dann erst wieder anmelden, wenn neue Mitarbeiter eingearbeitet werden müssen, wurde noch nie eine Cyber-Crucible-Funktion außer der Seite „Manage Agents“ genutzt. Wir helfen ihnen gerne dabei, die Ursachenanalyse (Root Cause Analysis) kennenzulernen – die für technisch versierte und halbtechnische Benutzer schmerzlos und einfach ist.

Die zweite Art von Kunden für die forensische Analyse nach einem Vorfall sind DFIR-Firmen, die zur Untersuchung eines Problems bei einem Kunden hinzugezogen werden, manchmal auf Anfrage der Cyber-Versicherung, und bei denen Cyber Crucible erst nach einem Vorfall installiert wird. (Nun, wir können nicht immer vor dem Angreifer da sein, so sehr wir das auch wollen … sonst hätte jedes Unternehmen der Welt uns bereits, und Erpressung wäre Geschichte!)

Die beste Beschreibung für eine Einführung nach einem Erpressungsangriff ist „chaotisch“. Nicht weil wir schwer zu installieren sind oder schwer mit dem Schutz beginnen können. Ganz im Gegenteil! In diesem Fall haben sich die Angreifer normalerweise bereits im System bewegt und sind in Betriebssysteme, Netzwerkgeräte, Active Directory eingebettet und arbeiten im Speicher. Bei mehreren Rechnern werden Prozesse beendet, und manchmal versuchen die Angreifer sogar, die Kontrolle zurückzugewinnen. Es ist ein wenig so, als würde man ein Medikament einnehmen, das einen zu Beginn krank macht, das man aber braucht, um wieder gesund zu werden.

Kunden, die bereits gestresst sind, reagieren manchmal emotional auf „mehr“ Lärm, wenn die Angreifer endlich aufgespürt und besiegt werden. Es ist viel Aufklärungsarbeit nötig, warum oder wie ihre bestehenden Sicherheitslösungen die Angreifer nicht gefunden haben. Am Ende gewinnt das Unternehmen jedoch wieder die Kontrolle über seine IT-Infrastruktur zurück. Sie werden nicht zu den 80–90 % der Unternehmen gehören, die ein oder zwei Jahre später erneut erpresst werden – in dem, was wir „die Erpressungs-Abo-Wirtschaft“ nennen.

Die dritte Art von Kunden, die wir haben, ist ein MSSP, der oft ein Partner von Cyber Crucible ist und auf einen automatisierten Schutz von Cyber Crucible reagiert. Sie müssen herausfinden, wie der Angreifer einen vorübergehenden Zugang erlangt hat, und alle Sicherheitslücken schließen. Die gute Nachricht ist, dass HIPAA- oder andere Compliance-Berichte aufgrund der Geschwindigkeit der automatisierten Reaktion typischerweise nur wenig oder gar keine Vertraulichkeitsverletzung ausweisen. Oft berichtet der MSSP „nichts zu melden“, was alle Beteiligten freut. Nun, außer den Kriminellen.

Revision #1
Created 2026-07-24 04:31:16 UTC by Dennis Underwood
Updated 2026-07-24 04:31:17 UTC by Dennis Underwood