REDMIMICRY

RedMimicry ist eine semi-automatisierte Lösung zur **Emulation von Cyberangriffen**. Sie ermöglicht es Ihnen, Cyberabwehrmaßnahmen gegen realistische Szenarien zu testen, die aktuellen Bedrohungen nachempfunden sind.

Die RedMimicry-Lösung bietet eine Vielzahl von Szenarien, von Malware bis hin zu gezielten Angriffen, die auf den **aktuellsten Taktiken und Methoden** basieren. Über eine benutzerfreundliche Weboberfläche können Sie alle Szenarien konfigurieren und steuern. Dadurch reduziert RedMimicry den sonst hohen manuellen Aufwand zur realistischen Nachstellung von Angreiferaktivitäten erheblich.

Einsatzmöglichkeiten

RedMimicry richtet sich an Unternehmen, die Endkunden beim **Aufbau von Fähigkeiten und Prozessen zur Cyberabwehr** unterstützen. RedMimicry kann sowohl zur Validierung bestehender Fähigkeiten und Prozesse als auch im Trainingskontext eingesetzt werden. Durch **Purple-Teaming** mit RedMimicry wird die Leistung von Cyber-Abwehrmaßnahmen effizient geprüft und verbessert, indem verschiedene Angriffsszenarien schrittweise durchgeführt und die Sichtbarkeit und Abwehrmaßnahmen beobachtet werden.

Anstatt nur isolierte Angriffsschritte zu testen, können Sie mit RedMimicry **mehrstufige und komplexe Bedrohungen** darstellen. RedMimicry emuliert relevante Techniken, Taktiken und Prozeduren (TTPs) sowie die eingesetzte Schadsoftware von realen Akteuren im Cyberraum, wie beispielsweise der Lockbit-Gruppe. Bei der Implementierung achten wir darauf, die für die Erkennung und Reaktion relevanten Details der nachgestellten Bedrohung möglichst genau nachzubilden. Die in RedMimicry-Playbooks eingesetzten Komponenten sind so implementiert, dass sie **sicher in Produktivnetzwerken** eingesetzt werden können.

Die Ausführung der Angriffe kann schrittweise erfolgen, sodass Sie nach jedem Schritt die Sichtbarkeit in überwachenden Systemen, wie **EDR und SIEM**, prüfen können. Alternativ ist auch eine automatische Ausführung der ganzen Angriffskette möglich. Die meisten Playbooks erlauben es Ihnen, manuell mit dem Zielsystem zu interagieren, eigene Befehle auszuführen oder zusätzliche Werkzeuge nachzuladen. Hierzu ist eine interaktive Shell implementiert.

Die RedMimicry GmbH konzentriert sich auf die Weiterentwicklung der Plattform und Playbooks. Eine **Begleitung bei den ersten Szenarien** und eine Schulung auf das System sind jedoch selbstverständlich möglich und empfohlen.

Vorteile

Realistisch: Anbieter von Red- und Purple-Teaming-Dienstleistungen greifen oft auf selbst entwickelte Lösungen zurück, die Open-Source-Komponenten mit Frameworks wie CobaltStrike, Nighthawk und Brute Ratel C4 kombinieren. Diese Lösungen haben jedoch den Nachteil, dass ihre Pflege und Dokumentation sehr aufwändig sind. Das führt oftmals zu Ressourcenkonflikten und beschränkt die Qualität und Quantität der verfügbaren Szenarien. RedMimicry stellt hingegen eine Bibliothek von realistischen Szenarien bereit, welche komplette Angriffsketten abbilden.

Wiederholbar: Mit RedMimicry benötigen Sie nur minimalen Aufwand, um weitere Endpunkte zu testen oder durchgeführte Tests zu wiederholen.

Nutzerfreundlich: Im Gegensatz zu Eigenentwicklungen ist die Benutzeroberfläche von RedMimicry auch für weniger erfahrene Anwender nutzbar und gut dokumentiert. Auch Junioren können komplexe Angriffe mit wenigen Mausklicks starten und orchestrieren.

Aktuell: RedMimicry bietet Updates für bestehende Playbooks und entwickelt kontinuierlich neue Szenarien. Damit stellen wir sicher, dass die durchgeführten Angriffe stets der aktuellen Bedrohungslage entsprechen.

Datensparsam: Sie können RedMimicry als On-Premises-Software nutzen. In diesem Fall werden keine Endkundendaten an die RedMimicry GmbH übertragen und Sie behalten die volle Kontrolle über laufende Szenarien. Dies erleichtert die Nutzung von RedMimicry auch in Unternehmen mit hohen Datenschutzanforderungen.

Kontakt

RedMimicry GmbH
Mahlower Straße 24
12049 Berlin
Germany

Stefan Steinberg
Chief Operating Officer
stefan.steinberg@redmimicry.com
+49 155 60175358