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

RedMimicry bietet eine Vielzahl von Szenarien, von Malware bis hin zu gezielten Angriffen, die auf den **aktuellsten Taktiken und Methoden** basieren. RedMimicry reduziert den sonst hohen manuellen Aufwand zur Nachstellung von **realistischen Angreiferaktivitäten** erheblich.

Einsatzmöglichkeiten

RedMimicry kann sowohl zur Validierung bestehender Fähigkeiten und Prozesse als auch für Trainings eingesetzt werden. Durch **Purple-Teaming** mit RedMimicry wird die Leistung Ihrer 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.

Vorteile

Realistisch: RedMimicry stellt eine ständig wachsende 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.

Datensparsam: RedMimicry kann on-premises betrieben werden. So werden keine Endkundendaten an die RedMimicry GmbH übertragen und Sie behalten die volle Kontrolle über laufende Szenarien.