LABYRINTH

Entwickelt, um fortgeschrittene Bedrohungen zu

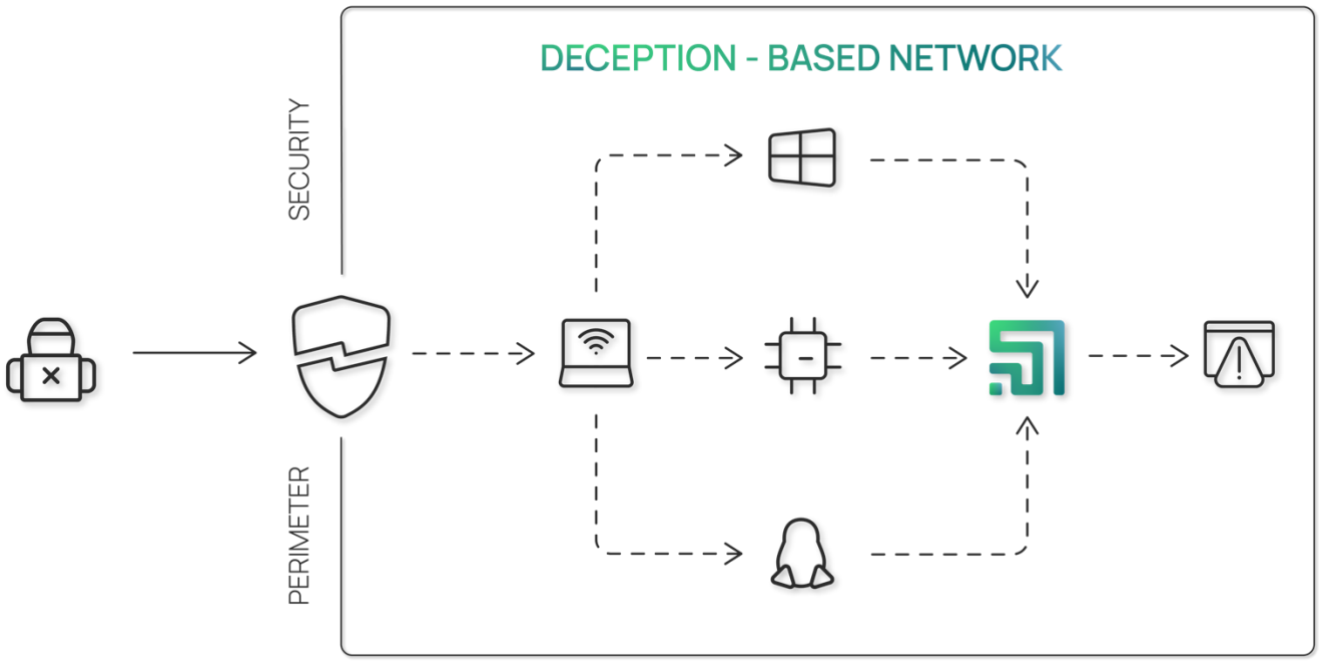
Beschreibung der Lösung

Labyrinth-Täuschungsplattform, 2023

Labyrinth ist eine auf Täuschung basierende Technologie zur Erkennung von Bedrohungen, die Cyberangriffe innerhalb eines Unternehmensnetzwerks identifiziert und blockiert. Unsere Lösung basiert auf einzigartigen Technologien zur Erkennung von Bedrohungen und schützt Ihr Netzwerk proaktiv vor gezielten Angriffen, fortgeschrittenen unbekannten Bedrohungen, Botnets, Zero-Day-Angriffen und böswilligen Insidern.

Die Plattform bietet ein einfaches und effizientes Tool für die frühestmögliche Erkennung von Angreifern innerhalb eines Unternehmensnetzwerks. Labyrinth lässt sich leicht in virtuellen, physischen oder hybriden IT-Umgebungen einsetzen und erkennt Bedrohungen, ohne dass eine kontinuierliche Überwachung erforderlich ist und Unmengen von Daten produziert werden.

Die Plattform bietet einen vollständigen Angriffszeitplan mit Ereigniskorrelation, um intelligentere und schnellere Entscheidungen zu treffen. Protection by Labyrinth gibt Ihnen die Gewissheit, dass Ihre wertvollen Daten vor Bedrohungen geschützt bleiben, die die Unternehmensfirewalls umgangen haben.



SCHLÜSSELFÄHIGKEITEN

Im Bereich der Cybersicherheit besteht eine bekannte Asymmetrie zwischen Angriff und Verteidigung: Die Verteidiger müssen zu 100 % richtig liegen, während die Angreifer nur einmal Glück haben müssen, um erfolgreich zu sein.
Die Labyrinth Deception Platform ist eine offensive Erkennungstechnologie, die das Gleichgewicht der Kräfte zugunsten der Verteidiger verschiebt. Die Plattform schaltet die Fähigkeit des Gegners zur Netzwerkaufklärung aus und verhindert so seitliche Bewegungen.

FRÜHZEITIGE NETZINTERNE ERKENNUNG VON BEDROHUNGEN

Labyrinth erkennt jede gezielte verdächtige Aktivität in einem frühen Stadium eines Angriffs. Labyrinth-Punkte (Netzwerkköder) sind so konzipiert, dass sie Bedrohungsaktionen abfangen, wenn ein Angreifer versucht, das Netzwerk zu verstehen und sein Ziel zu finden.
Sobald ein Angreifer einen Punkt angreift, sammelt Labyrinth alle Details über ihn: die Quellen der Bedrohung, die verwendeten Tools und die ausgenutzten Schwachstellen. Gleichzeitig arbeiten alle realen Anlagen und Dienste ohne jegliche Beeinträchtigung.

GENAUE WARNUNGEN

Labyrinth unterstützt Sicherheitsteams mit äußerst zuverlässigen Alarmen mit weniger als 1 % Fehlalarmen. Labyrinth-Punkte sind von Natur aus still, bis sie berührt werden. Niemand soll mit ihnen in Kontakt treten, so dass jede Interaktion mit einem Punkt besonders verdächtig ist. Dies unterscheidet Labyrinth von Sicherheitslösungen, die alle Aktivitäten in einem Netzwerk analysieren sollen und eine Menge digitales "Rauschen" erzeugen.

SCHNELLE REAKTION AUF ZWISCHENFÄLLE

Labyrinth bietet ein intelligentes Analyseinstrument für die Untersuchung von Vorfällen und die Identifizierung von Bedrohungen. Alle erfassten Ereignisse werden mit den notwendigen Sicherheitsdaten aus der Incident Response Platform angereichert.
Die von Labyrinth generierten Indicators of Compromise (IoC) werden automatisch mit den Threat Prevention-Lösungen synchronisiert. Dies ermöglicht es, sofort Maßnahmen gegen Angriffe zu ergreifen: sie zu verstehen, forensisch zu untersuchen, zuversichtlich zu reagieren und eine bessere Verteidigung für die Zukunft zu entwickeln.

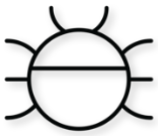
PROAKTIVE VERTEIDIGUNG

Die meisten Erkennungstechnologien stoppen einen Angriff, sobald sie ihn entdeckt haben, und geben keine Gelegenheit, ihn zu untersuchen. Wichtige Informationen, die zur Beseitigung eines Angriffs beitragen und verhindern, dass dieser Angriff wiederkehrt, gehen verloren.
Labyrinth ermöglicht es, mehr über die Art eines Angriffs zu erfahren und die von Angreifern verwendeten Werkzeuge und Techniken besser zu verstehen. Die Lösung generiert und installiert Täuschungsartefakte, deren Ziel es ist, Angreifer mit einer verlockenden Fälschung zu locken. Anstatt einfach abzuwarten, was ein Angreifer als Nächstes tun wird, leiten die Artefakte ihn in eine isolierte Umgebung, die er beobachten kann.

GEZIELTE ANGRIFFE ZUR AUFDECKUNG

Um wirksam gegen gezielte Angriffe vorgehen zu können, ist es entscheidend, die Techniken, Werkzeuge und Ziele der Angreifer zu verstehen.
Die Labyrinth Deception Platform lockt Hacker oder böswillige Insider in ein falsches Gefühl der Sicherheit und ermöglicht es ihnen, ihre Fähigkeiten und Motive zu lernen. Das Wissen darüber, was Angreifer über Unternehmensnetzwerke, Anwendungen und Mitarbeiter wissen, hilft dabei, ein möglichst genaues Profil der Angreifer zu erstellen und die bestmögliche Verteidigung gegen sie anzuwenden. Außerdem werden Schwachstellen in den Verteidigungssystemen von Unternehmen aufgedeckt, die von Angreifern in Zukunft ausgenutzt werden können.

ERKENNUNG NACH DER INFEKTION

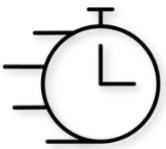


Die Labyrinth Deception Platform, die in den Netzwerken eines Unternehmens implementiert ist, kann als äußerst zuverlässiges Alarmsystem für Angriffe dienen, die die Sicherheitskontrollen am Netzwerkrand umgangen haben.
Seeder-Agenten, die auf Servern und Workstations eingesetzt werden, imitieren die für Angreifer "leckersten" Artefakte. Was wie ein hoch privilegiertes und schlecht geschütztes Administratorkonto aussieht, ist eine Falle, die einen Angreifer ins Labyrinth lockt. Dort können Sie die Aktionen der Angreifer im Umgang mit Points überwachen und wertvolle Erkenntnisse über Bedrohungen sammeln, die die Perimeter-Verteidigung durchdrungen haben.

ERKENNUNG VON QUERBEWEGUNGEN

In der Phase der lateralen Bewegung bewegt sich ein Angreifer in einem Unternehmensnetzwerk von einer Anlage zu einer anderen. Die Labyrinth Deception Platform wurde entwickelt, um die frühe Aufklärung, den Diebstahl von Zugangsdaten und laterale Bewegungen zu erkennen.
Es ermöglicht Unternehmen, solche Bedrohungen in einem frühen Stadium zu erkennen, was für herkömmliche Sicherheitslösungen eine komplizierte Aufgabe ist. Labyrinth zeigt den nächsten Schritt eines Angriffs auf das Täuschungsökosystem und entlarvt einen Angreifer sofort.

REDUZIERUNG DER VERWEILZEIT



Der Labyrinth-Erkennungsmechanismus ist besonders effizient, wenn es darum geht, die Verweildauer zu verkürzen, d. h. die Zeit, in der ein Angreifer innerhalb eines Unternehmensnetzes unbemerkt bleibt. Eine lange Verweildauer ist eine entscheidende Voraussetzung dafür, dass ein Angreifer einen Angriff erfolgreich abschließen kann. Labyrinth verkürzt die Verweildauer von Angriffen, indem es Honeypots, Köder und Breadcrumbs für Angreifer einrichtet. Die Labyrinth Deception Platform verkürzt die Zeit und die Möglichkeiten von Angreifern, sich in Unternehmensnetzwerken zu bewegen und stoppt sie, bevor sie kritische Anlagen und Dienste erreichen.

UNTERNEHMENSWERTE

NULL-LEISTUNG IMPACT

Keine negativen Auswirkungen auf die Leistung von Netzwerkgeräten, Hosts, Servern oder Anwendungen.

FORTGESCHRITTENE BEDROHUNGEN ZU STOPPEN

Entdeckt gezielte und fortgeschrittene Angriffe
ohne jegliche Vorkenntnisse
der Form, der Art oder des Verhaltens der Bedrohung.
Die Plattform erkennt bekannte und unbekannte Bedrohungen in der frühesten Phase des Lebenszyklus eines Angriffs.

BETRIEBSKOSTEN SENKEN

Er sammelt keine Unmengen von Daten,
keine falsch-positiven Alarme erzeugen,
für die Bedienung sind keine besonderen Kenntnisse erforderlich.

Es lässt sich problemlos in bestehende Sicherheitsinfrastrukturen einbinden und erzeugt keine Fehlalarme.

AUTOMATISIERTES GESCHEHEN ANTWORT

Er sammelt keine Unmengen von Daten,
keine falsch-positiven Alarme erzeugen,
für die Bedienung sind keine besonderen Kenntnisse erforderlich.

Es lässt sich problemlos in bestehende Sicherheitsinfrastrukturen einbinden und erzeugt keine Fehlalarme.

MINIMUM HANDBUCH KONFIGURATION

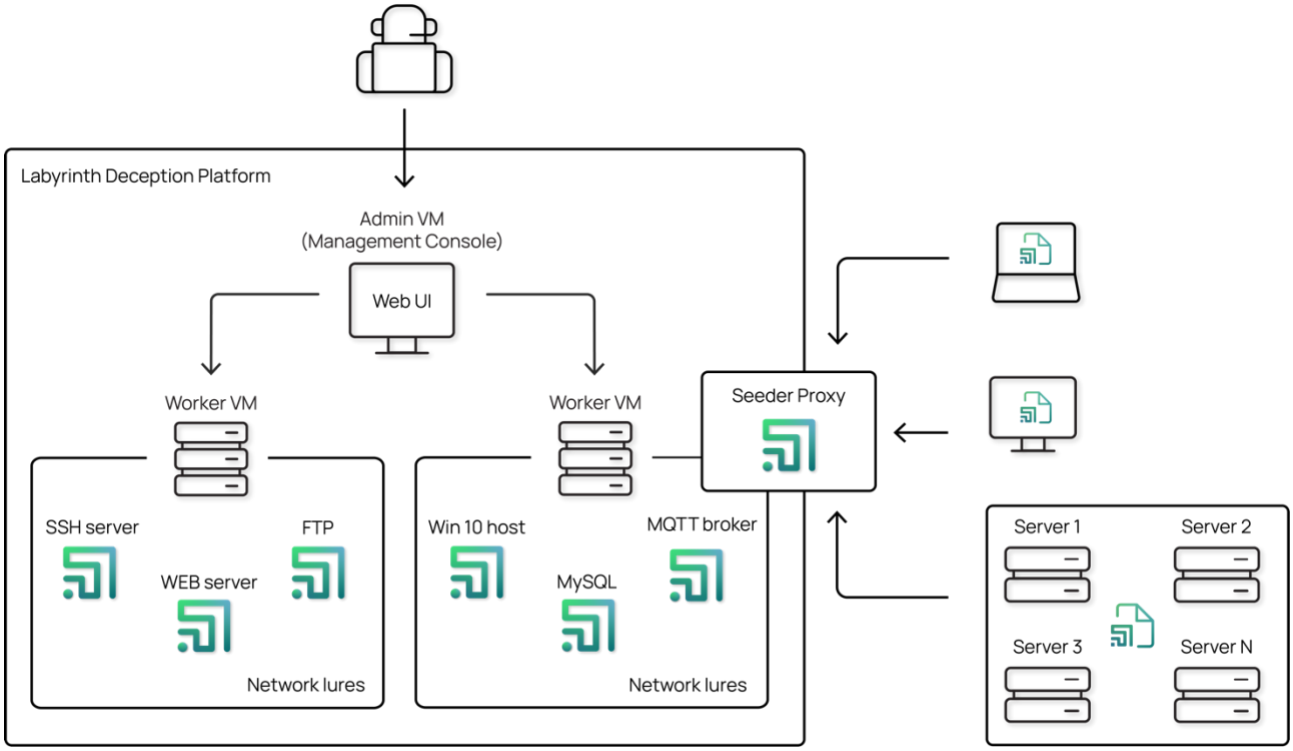
Schnelle und einfache Einführung ohne Systemkonflikte und mit minimalem Wartungsaufwand:
keine Datenbanken, Signaturen oder Regeln
zu konfigurieren und zu aktualisieren.

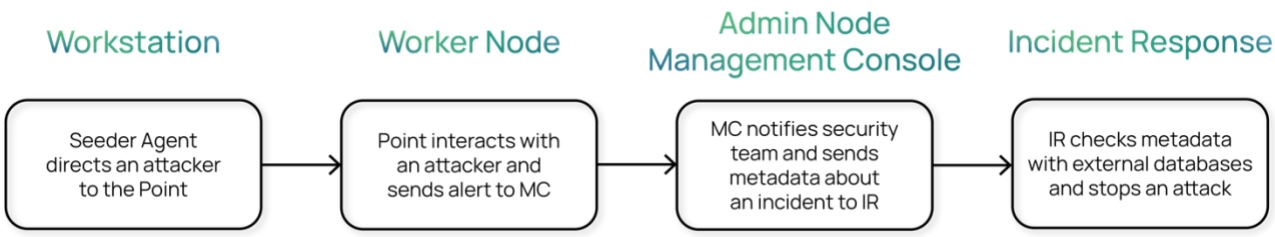
ARCHITEKTUR

Die Labyrinth Plattform setzt automatisch Honeynets ein, basierend auf den Informationen über die Netzwerkumgebung und die verwendeten Geräte. Decoys können auch manuell über die Management-Konsole eingesetzt werden.

Sie gibt Unternehmen ein leistungsfähiges Werkzeug an die Hand, um ihre eigene, einzigartige Deception Platform zu entwickeln, die auf ihren speziellen Bedürfnissen und globalen Best Practices basiert.

Die Plattform bietet Angreifern eine Illusion von IT-Diensten und Anwendungsschwachstellen, provoziert sie zu Aktionen, erkennt und überwacht alle ihre Aktivitäten und isoliert sie vom realen IT-Netzwerk.





KEY FEATURES

Die Labyrinth Deception Platform emuliert keine reale IT-Infrastruktur. Stattdessen bietet die Plattform Angreifern eine Illusion von realen IT-Netzwerkschwachstellen. Das Labyrinth Technology Team aktualisiert die Lösung kontinuierlich mit Imitationen von neu entdeckten Schwachstellen. Das macht Labyrinth zu einem sehr effizienten Werkzeug für die Erkennung und Abwehr fortgeschrittener Bedrohungen.

HONEYPOTS MIT HOHER INTERAKTION

Die Labyrinth Deception Platform basiert auf Points - Honeypots mit hoher Interaktion und intelligenten Funktionen. Die Points sind identisch mit den Unternehmensressourcen und führen echte Betriebssysteme, Anwendungen und Dienste mit gefälschten Daten aus.

Sie ermöglichen es einem Angreifer, sich einzuloggen und auf seine Anfragen zu reagieren, um seine Absichten zu verstehen. Points locken sie für eine lange Zeit an, beobachten sie und sammeln wertvolle Daten über ihre Tools und Techniken. Darüber hinaus erzeugen Points lokale Indikatoren für die Gefährdung (Indicators of Compromise, IoCs) und maschinenlesbare Bedrohungsdaten (Machine Readable Threat Intelligence, MRTI).

PUNKTE VIELFALT UND AUTHENTIZITÄT

Labyrinth Points spiegeln Schwachstellen in Produktionsnetzwerken wider und emulieren reale Betriebssysteme/Images, Dienste und Anwendungen für IoT, SCADA/OT, POS, ICS, Netzwerk- und Telekommunikationsumgebungen. Falsche Workstations, Server, Geräte, Anwendungen, Dienste und Protokolle sehen identisch aus wie echte Anlagen.

Labyrinth Points emulieren nicht nur die für Angreifer attraktivsten Schwachstellen, sondern verhalten sich auch wie echte Hosts. Je nach Typ können sie Broadcast-Anfragen senden, IP-Adressen ändern und Verbindungen zu Nachrichten-Websites herstellen. Es ist möglich, Köder in eine Produktionsumgebung einzubauen und sie von den übrigen Assets abzuheben, um als Ziel für einen Angreifer ausgewählt zu werden.

MEHRSCHICHTIGE SICHERHEIT

Labyrinth implementiert ein vollständiges Täuschungskonzept, um seinen Kunden ein Höchstmaß an Sicherheit zu bieten. Artefakte mit geringer Interaktion in der ersten Verteidigungslinie emulieren Unternehmensanwendungen und werden nur für die grundlegende Erkennung von Bedrohungen verwendet.

Sie sind leicht zu entdecken und zu umgehen und zeigen Angreifern, dass sie sich in einem Minenfeld befinden. Sie schrecken opportunistische Angreifer ab und geben gezielten Angreifern das falsche Vertrauen, dass sie Täuschungen in einem Netz entdeckt haben. In der Zwischenzeit bleiben hochinteraktive Täuschungsmanöver unbemerkt und gewährleisten die Erkennung fortgeschrittener Bedrohungen.

CUSTOMIZATION

Das Labyrinth Deception Team bietet fortschrittliche Dienstleistungen zur Entwicklung von Labyrinth in komplexen Umgebungen oder für spezielle Branchenanforderungen wie IoT, SCADA oder POS. Unsere Cybersicherheitsspezialisten arbeiten ständig daran, neue Bedrohungen zu finden/aufzudecken. Nach der Analyse entwickeln wir neue Labyrinth-Pfade und Punkte, um die Aktivitäten der Bedrohung zu täuschen.

Jede Labyrinth-Installation aktualisiert ihre Karte regelmäßig mit neuen Pfaden und Punkten, um die besten Täuschungsmöglichkeiten zu bieten. Um die Verteidigung zu stärken, wenn ein Angriff im Gange ist, können zusätzliche Punkte hinzugefügt oder die Typen der Punkte geändert werden.

AUTOMATION

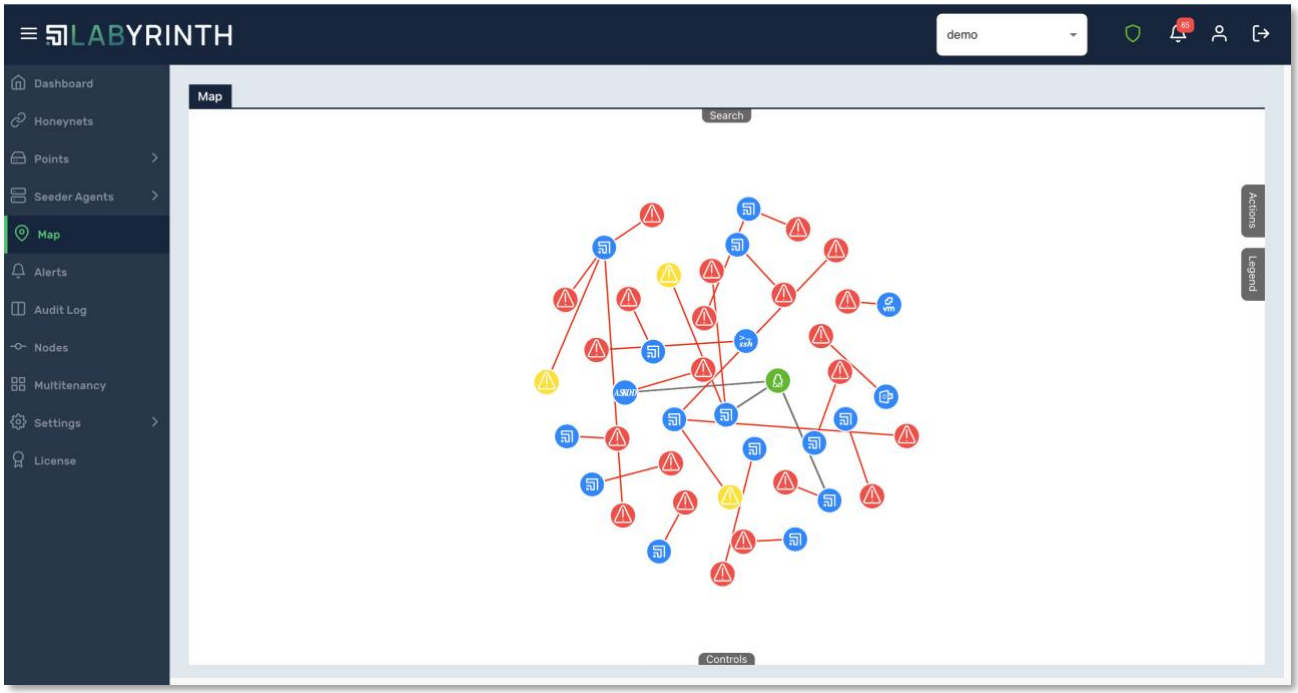
Die Labyrinth Deception Platform identifiziert automatisch Hosts, Services und Verbindungswege zwischen ihnen, um die Erstellung und den Einsatz von Täuschungsmanövern und Honeypots zu optimieren und anzupassen.

Die fortschrittlichen Netzwerkfunktionen bieten die Möglichkeit, dynamisch neue Pfade in Labyrinth zu erstellen und Punkte zu aktualisieren. Labyrinth bietet eine automatisierte Verwaltung und regelmäßige Aktualisierung der in der Produktionsumgebung installierten Punkte, um die Authentizität zu erhalten. Die leichtgewichtige, automatisierte und flexible Lösung spart Zeit und bietet ein hohes Maß an Sicherheit vom ersten Tag der Bereitstellung an.

SKALIERBARKEIT

Labyrinth kann in großen verteilten Unternehmensnetzen effizient skaliert werden. Jeder emulierte Punkt ist ein leichtgewichtiger Prozess, der auf einer virtuellen Maschine läuft. Die Skalierbarkeit von Labyrinth hängt also nicht von den Verarbeitungsressourcen ab, sondern basiert auf der Konstruktion und Implementierung einer umfassenden und realistischen Reihe von Täuschungsmanövern und Honeypots in der gesamten Netzwerkumgebung.

Die automatische Erstellung und Bereitstellung von Punkten hilft Unternehmen, einen Skalierungsprozess zu rationalisieren und einen vollständigen Schutz aller Netzwerksegmente zu erreichen.



Die Labyrinth Deception Platform bietet das effizienteste Werkzeug, um die Bewegungen von Hackern innerhalb des Unternehmensnetzwerks zu erkennen und zu stoppen.

Für weitere Informationen über Labyrinth oder für eine Produktvorführung kontaktieren Sie uns bitte unter **info@labyrinth.tech**