Die Labyrinth Deception Platform verändert eine Angriffsfläche, die Angreifern die Illusion echter Infrastrukturschwachstellen vermittelt. Jeder Teil der nachgeahmten Umgebung reproduziert die Dienste und Inhalte eines echten Netzwerksegments. Die Lösung basiert auf Points - intelligenten Imitationshosts, die spezielle Softwaredienste, Inhalte, Router, Geräte usw. nachahmen. Die Punkte erkennen alle bösartigen Aktivitäten innerhalb eines Unternehmensnetzes und decken alle möglichen Angriffsvektoren ab.

Labyrinth provoziert den Angreifer zu Aktionen und erkennt verdächtige Aktivitäten. Während sich ein Angreifer durch die gefälschte Zielinfrastruktur bewegt, erfasst die Plattform alle Details des Angreifers. Das Sicherheitsteam erhält Informationen über die Quellen der Bedrohung, die verwendeten Tools, die ausgenutzten Schwachstellen und das Verhalten des Angreifers.

Vorteile der Labyrinth Täuschungsplattform

- Erkennt und stoppt gezielte und fortschrittliche Cyberangriffe, ohne dass vorherige Kenntnisse über
  der Form, der Art oder des Verhaltens der Bedrohung.
- Reduziert die Betriebskosten für die Cybersicherheit um bis zu 30 %: Es werden keine Unmengen von Daten gesammelt, es gibt keine Fehlalarme, und es sind keine besonderen Kenntnisse erforderlich.
- Beschleunigt die Reaktion auf Vorfälle, indem es die durchschnittliche Zeit für die Erkennung und Reaktion auf Bedrohungen (MTTD, MTTR) um das 12-fache reduziert.
- Keine negativen Auswirkungen auf die Leistung von Netzwerkgeräten, Hosts, Servern oder Anwendungen.
- Schnelle und einfache Bereitstellung, keine Systemkonflikte und kein Wartungsbedarf - keine Datenbanken, Signaturen oder Regeln, die ständig konfiguriert und aktualisiert werden müssen.

Vorteile gegenüber anderen Ansätzen zur Erkennung von Cyber-Bedrohungen

Erweiterte Erkennung von Bedrohungen

- Ermöglicht es Ihnen, Eindringlinge in Ihrem Unternehmensnetzwerk bis zu 12 Mal schneller zu erkennen
- Erkennt grundlegende und fortgeschrittene Bedrohungen unabhängig von den verwendeten Methoden
- Sammelt Daten über die Bewegungen von Angreifern und die von ihnen verwendeten Tools

Prozessoptimierung für SOC

- Erhebliche Vereinfachung des Prozesses der Priorisierung von Vorfällen
- Verringert den Zeitaufwand für Falsch-Positiv-Meldungen
- Bietet vollständige Transparenz des Angriffs in Echtzeit

Keine tiefgreifenden Kenntnisse erforderlich

- Einfache Installation und Einrichtung
- Für die Nutzung der Lösung sind keine besonderen Kenntnisse erforderlich

- Automatische Erkennung von und Reaktion auf Vorfälle bei Integration mit Tools von Drittanbietern

Technische Vorteile gegenüber anderen Deception-Lösungen

- Im Gegensatz zu anderen Deception-Lösungen verwendet die Labyrinth-Plattform komplexe Methoden zur Erkennung und Verhinderung von Angriffen, die von Menschen durchgeführt werden. Dieser Ansatz umfasst und implementiert nicht nur Deception-Methoden, sondern auch eine breite Palette anderer Tools zur Erkennung komplexer Cyberbedrohungen.
- Alle von Labyrinth erstellten Simulationen haben einen hohen Interaktionsgrad, d. h. sie reagieren zumindest auf die Interaktivität beim Scannen, fordern zur Eingabe von Anmeldeinformationen auf und zeigen eine grafische und/oder textuelle Schnittstelle an. Jeder Hook ist einzigartig, mit einer IP-Adresse; es wird kein IP-Alias verwendet. Dieser Ansatz bietet die branchenweit beste Glaubwürdigkeit für die erstellten Simulationen.
- Universal Web Point ist eine einzigartige Art von Trap. Das System scannt Ihr Netzwerk und verwendet die gesammelten Informationen, um automatisch Emulationen lokaler Web-Ressourcen des Netzwerks mit dem Zusatz von Schwachstellen und der Möglichkeit, diese auszunutzen (Scan-Antworten, Anforderung von Anmeldeinformationen, Anzeige einer grafischen Oberfläche) zu erstellen.

Erweiterte Systemfunktionen:

- Multitenancy - ermöglicht die Isolierung und Bedienung von Benutzern aus verschiedenen Organisationen in einer Installation (MSSP-Ansatz).
- Zwei-Wege-Integration mit SIEM-Lösungen, die es nicht nur ermöglicht, Daten an SIEMs zu senden, sondern auch notwendige Informationen von ihnen zu erhalten.
- Aktive Täuschungsmanöver zur Erkennung von MiTM-Angriffen (Man-in-the-Middle).

Kommerzielle Vorteile gegenüber anderen Deception-Lösungen

- Branchenführende Time-to-Value: Der gesamte Systembereitstellungsprozess von der Inbetriebnahme bis zur Produktion dauert nur wenige Stunden.
- Für die volle Funktionsfähigkeit des Systems ist kein zusätzlicher Erwerb von Softwarelizenzen Dritter (z. B. Windows) erforderlich.
- Für die Bereitstellung des Systems sind keine großen Hardwareressourcen erforderlich.
- Unterstützt die Hypervisoren VMWare und Hyper-V.
- Flexible Lizenzierung je nach Infrastrukturgröße und Kundenanforderungen.
- Die Lizenzierung erfolgt nicht nach der Anzahl der Breadcrumbs, Endpunkte, etc. - in der Praxis wird nur die Anzahl der Netzwerksegmente lizenziert. Jedes Segment kann bis zu 15 Points (Decoys) einsetzen.
- Die Preise für die Lösung sind wesentlich günstiger als die von den Wettbewerbern angebotenen.