



HIGHEND
DECEPTION
TECHNOLOGY
SOLUTION



CyberTrap

We know your enemies

WARUM HERKÖMMLICHE IT SICHERHEIT NICHT LÄNGER AUSREICHT

PRÄVENTION VERSAGT

Anti-Virus Lösungen, Intrusion Detection Systeme sowie weitere Verteidigungsmechanismen bilden einen unverzichtbaren Basisschutz gegen das Grundrauschen des Internets, können professionellen Angreifern jedoch nur wenig entgegensetzen.

Im Gegensatz zu "altmodischen" Bedrohungen kämpfen Unternehmen heutzutage nicht mehr ausschließlich gegen gewöhnliche Viren, sondern auch gegen professionelle, hoch motivierte Individuen mit krimineller Absicht und einer klar definierten Mission: die Kronjuwelen ihrer Organisation zu stehlen!

Die Angreifer haben Ihre Organisation aus einem bestimmten Grund als Ziel ausgewählt, sie besitzen ausreichend Mittel, sind gut organisiert, motiviert und sehr gut ausgebildet. Maßgeschneiderte und zielgerichtete Angriffe auf Ihre Organisation sind unvermeidbar. Die Herausforderung ist es, die Zeit, in der sich ein Angreifer tatsächlich unbemerkt im eigenen Unternehmen aufhält, so weit als möglich zu reduzieren. Daher wird laufendes Monitoring und schnelles Reagieren bei einem erfolgreichen Angriff zunehmend geschäftskritisch.

CYBERTRAP

CyberTrap ändert die Spielregeln: Als eine fortschrittliche hoch interaktive Deception Technology (Täuschungstechnologie) lockt CyberTrap die Angreifer in eine digitale Spielwiese.

Mittels Live-Analyse ermöglicht dies Organisationen zum ersten Mal einen detaillierten Einblick in die Vorgehensweisen von Eindringlingen und damit auch volle Kontrolle über diesen Einbruch.

Das Verständnis über die Vorgehensweisen eines Angreifers ist essentiell, denn es ermöglicht:

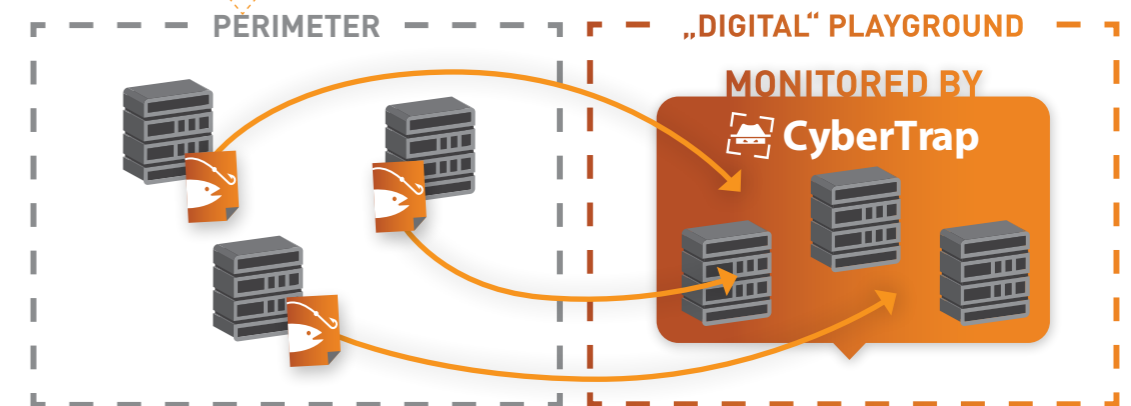
- die aktuelle Bedrohungslage und Risikolandschaft einzuschätzen
- effiziente Auswahl von Sicherheitsmaßnahmen zu treffen
- zu agieren bevor der Angreifer auf wertvolle Kronjuwelen stößt

Indem einzigartige lokale Threat Intelligence gesammelt wird ermöglicht CyberTrap:

- die Absichten des Angreifers zu verstehen
- Informationen über Malware, Angreifer-Tools und zahlreiche Fingerprints in Echtzeit zu sammeln
- Angreifer persönlich mithilfe der CyberTrap TrackDown Dokumente zu identifizieren
- die Infrastruktur des Angreifers zu attributieren und darzustellen
- die aktuelle Bedrohungslage der produktiven Umgebung zu evaluieren
- die Effektivität und das Investment in bestehende Sicherheitslösungen mittels Einspielung der Daten der gesammelten lokalen Threat Intelligence signifikant zu steigern

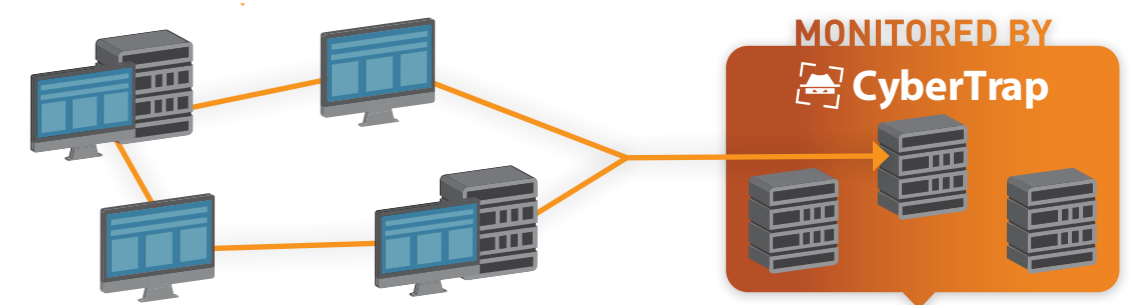
BETRIEBSSZENARIOEN

DMZ INTEGRATION



Stand-alone oder integriert mittels Köder in eine bestehende Web-Applikation. Ermöglicht die **Erkennung von klassischen externen Angriffen sowie hoch entwickelten Bedrohungen (advanced threats).**

INTRANET & END POINT INTEGRATION



Agentless **Integration von Ködern in Endgeräte** zur Identifikation von hoch entwickelten Bedrohungen (APT), Insidern oder Ransomware.

TRACKDOWN DOKUMENTE

Bösartige Aktivitäten wie Betrug, Erpressung oder Spionage sind eine wachsende Bedrohung für Organisationen. Ausserdem gibt es kaum technische Möglichkeiten diesen Akteuren das Handwerk zu legen. TrackDown Dokumente ändern dieses Dilemma indem sie für den Angreifer nicht erkennbare High-Tech Gegenmaßnahmen setzen. Virtuelle Peilsender in präparierten Dokumenten haben sich als höchst effektiv im Kampf gegen solche Betrüger herausgestellt. Es kann dabei nicht nur der Täter persönlich identifiziert werden, sondern auch etwaige Hintermänner.



FEATURES

| |
|--|
| Full Deception Stack (Daten, Applikation, Endpoint, Netzwerk) |
| Basierend auf echten Betriebssystemen und Applikationen |
| Störungsfreie, ressourcenschonende Implementierung |
| TrackDown Dokumente |
| Echtzeiterkennung |
| Angreiferattributierung |
| Live Angriffsanalyse |
| Agentenlose Integration in Webapplikationen und Endgeräte |
| Lokale Threat Intelligence (bis zu TTP Level!) |
| Erkennung von Zero Days |

BETRIEBSMODELL

CyberTrap kann on-premise oder in der Cloud betrieben werden.

| | Self-Managed | Managed |
|--|--------------|---------|
| CyberTrap SaaS | x | x |
| Wartung & Updates | x | x |
| Monitoring durch CyberTrap Operation Center | | x |
| Angreiferattributierung | x | x |
| In-Depth Analysis durch Security Analysts | | x |
| Intelligence Reports | | x |
| Automatische Reporting | x | x |
| Alarmierung | x | x |



Kontakt Daten:

CyberTrap Software GmbH

Komarigasse 14/1

2700 Wiener Neustadt

sales@cybertrap.com

www.cybertrap.com