

PRÄVENTION ALLEIN REICHT NICHT

LABYRINTH erkennt Angreiferaktivitäten, die klassische Präventionsmaßnahmen nicht verhindern.

MAKE HACKERS CRY



WAS KLASSISCHE PRÄVENTION ÜBERSIEHT

Jetzt gerade könnte ein Angreifer in Ihrem Netzwerk unterwegs sein. Wüssten Sie davon? Angreifer nutzen legitime Zugriffswege, vertrauenswürdige Prozesse und gültige Sessions. Damit umgehen sie regelbasierte Erkennung.

LABYRINTH macht diese Aktivitäten sichtbar, bevor Angreifer ihr eigentliches Ziel erreichen.

29min

Durchschnittliche Zeit vom
initialen Zugriff bis zur
aktiven Ausbreitung

56%

aller Sicherheitsverletzungen
bleiben mindestens einen
Monat unentdeckt

<1%

False-Positive-Rate mit
LABYRINTH

BEHÖRDEN & VERTEIDIGUNG

GESUNDHEITSWESEN

FINANZWESEN

KRITISCHE INFRASTRUKTUR (KRITIS)

HANDEL

LOGISTIK

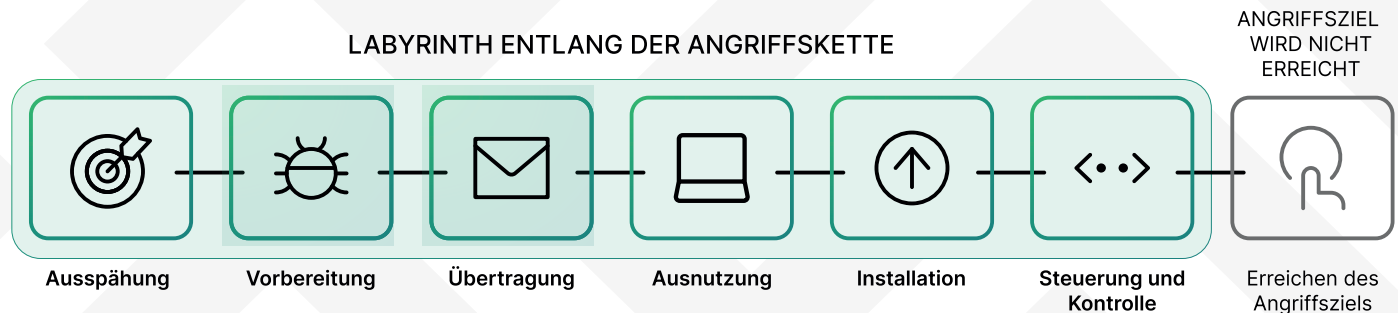
ENERGIE

TELEKOMMUNIKATION

SCHUTZ IN ALLEN ANGRIFFSPHASEN

Angriffe verlaufen in mehreren Phasen: von der ersten Recherche zu einem potenziellen Ziel bis zur eigentlichen Attacke.

LABYRINTH deckt den gesamten Angriffsverlauf ab. Die einzelnen Funktionen greifen dabei an unterschiedlichen Stellen ineinander.



VIER FUNKTIONEN. EIN DURCHGÄNGIGER SICHERHEITSANSATZ.

Dark Web Monitoring, Advanced Deception, Seeker und Threat Intelligence greifen an unterschiedlichen Punkten des Angriffsverlaufs ineinander:

DARK WEB MONITORING

Überwacht Dark-Web-Quellen auf kompromittierte Zugangsdaten, offengelegte Daten und frühe Anzeichen gezielter Kampagnen.

Ziel: Frühzeitige Transparenz über potenzielle Angriffe, bevor die eigene Umgebung betroffen ist.

ADVANCED DECEPTION

Bildet reale Assets durch realistische Decoys, Services und Artefakte in IT-, OT- und Cloud-Umgebungen nach. Jede unautorisierte Interaktion löst einen High-Confidence Alert aus.

Ziel: Angreiferaktivitäten unmittelbar erkennen.

SEEKER

Simuliert kontinuierlich Angreiferverhalten und überprüft Security-Kontrollen, -Richtlinien sowie die Reaktionsfähigkeit des Security-Teams.

Ziel: Fehlkonfigurationen und Kontrolllücken erkennen, bevor reale Angreifer sie ausnutzen.

THREAT INTELLIGENCE

Analysiert erfasste Angreiferaktivitäten und liefert konkrete Erkenntnisse zu Verhalten, Mustern und zusammenhängenden Interaktionen. Gewonnene Artefakte können genutzt werden, um die Angriffserkennung gezielt weiterzuentwickeln.

Ziel: Angriffe besser verstehen und die Erkennung zukünftiger Bedrohungen verbessern.

IN EUROPA ENTWICKELT. UNTER REALEN BEDINGUNGEN ERPROBT.

LABYRINTH ist ein 2019 gegründetes Cybersecurity-Unternehmen mit Hauptsitz im polnischen Zabrze. Die Deception-Technologie wurde ursprünglich in der Ukraine entwickelt und unter realen Cyberangriffen erprobt. Heute gilt LABYRINTH als führender europäischer Anbieter für Cyber Deception und Preemptive Cybersecurity.

LABYRINTH trägt das Label „**Cybersecurity Made in Europe**“, ist Mitglied des **CyberMadeInPoland** Clusters und liefert **souveräne europäische Cybersicherheit** an Kunden weltweit. Die vollständig selbst gehostete Lösung verfolgt einen strategischen Ansatz für Preemptive Cybersecurity: Bedrohungen frühzeitig erkennen, bevor sie Schaden verursachen, ohne zusätzliche operative Komplexität für Security Teams.

