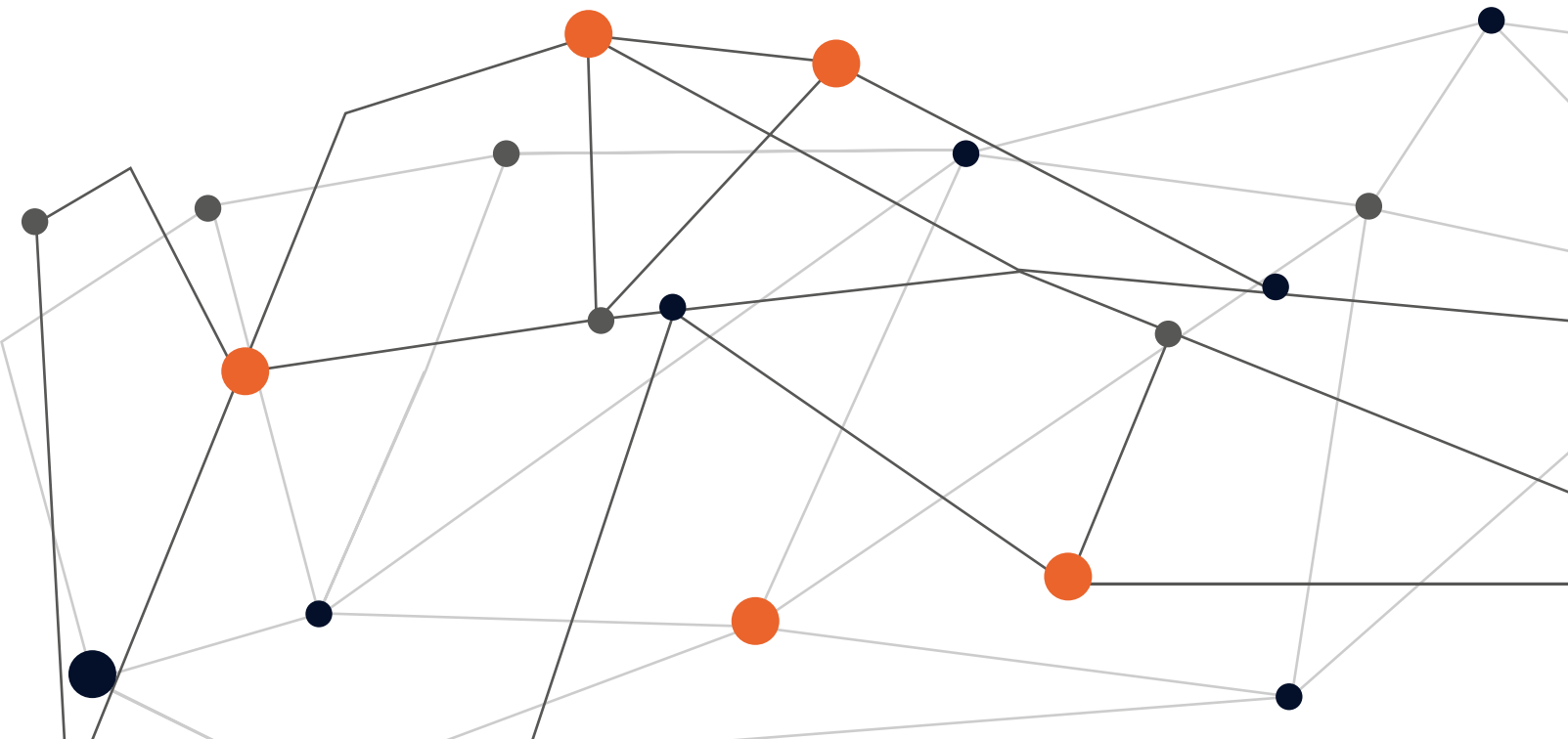
# CYBERSENSE

## ADVANCED DECEPTION TECHNOLOGY AS A MANAGED SERVICE



# CYBERSENSE

## ADVANCED DECEPTION TECHNOLOGY AS A MANAGED SERVICE

## » EINBRUCHSERKENNUNG EINFACH UND **WIRKSAM**

Der **CYBERSENSE MANAGED SERVICE** erkennt Einbrüche in Ihr Unternehmensnetzwerk einfach und wirksam. Cybersense basiert auf einem komplementären Ansatz, der unabhängig von vorhandenen Sicherheitssystemen funktioniert. Während seiner Erkundungsphase nutzt der Angreifer präparierte Informationen, deren Nutzung sofortigen Alarm auslöst. Der Angreifer hat keine Chance zu erkennen, ob er echte, wertvolle Daten oder von Cybersense vorgetäuschte Informationen erbeutet hat.

## » EINBRÜCHE ERKENNEN **BEVOR** SCHADEN ENTSTEHT

Schaden entsteht, weil erfolgreiche Angriffe nicht oder zu spät entdeckt werden. Im Durchschnitt bewegen sich Angreifer 6 Monate unbemerkt in Unternehmensnetzwerken. Mit viel Kreativität und Einfallsreichtum überwinden sie immer wieder innovative und intelligente Sicherheitssysteme. Die Zahl erfolgreicher Angriffe steigt trotz aller Gegenmaßnahmen

**68%**

aller Einbrüche werden erst nach Wochen oder Monaten entdeckt.

(Quelle: Verizon, Data Breach Investigations Report 2018, Seite 6)

**176**

Tage dauert es in Europa im Schnitt bis ein Einbruch entdeckt wird.

(Quelle: FireEye Mandiant, M-Trends Report 2019, Seite 6)

## » DAS **VORGEHEN** VON ANGREIFERN

Die meisten Einbrüche basieren nicht auf den berüchtigten, hochkomplexen Angriffen. Vielmehr stehen dem Angreifer alle digitalen, sozialen oder physischen Methoden zur Verfügung, um sich einen ersten Eintrittspunkt zu verschaffen. Hier ist der Angreifer klar im Vorteil. Hat er erst einmal Zugang bekommen - meist mit geringen Nutzerrechten - versucht er, unter Nutzung einschlägiger Angriffstools, seine Befugnisse im Unternehmensnetz zu erweitern und seine Spuren zu verwischen. Hier ist die Schwachstelle des Angreifers, die sich Cybersense zunutze macht. Er befindet sich in einem ihm vollkommen unbekannten Netzwerk und muss diese Umgebung zuerst erkunden. Zwar wird der Angreifer sehr vorsichtig vorgehen, aber letztlich muss er die wenigen erbeuteten Informationen nutzen, um mehr Informationen zu bekommen. Cybersense infiltriert diesen Erkundungsprozess und bietet vorgetäuschte Informationen, die sofortigen Alarm auslösen.

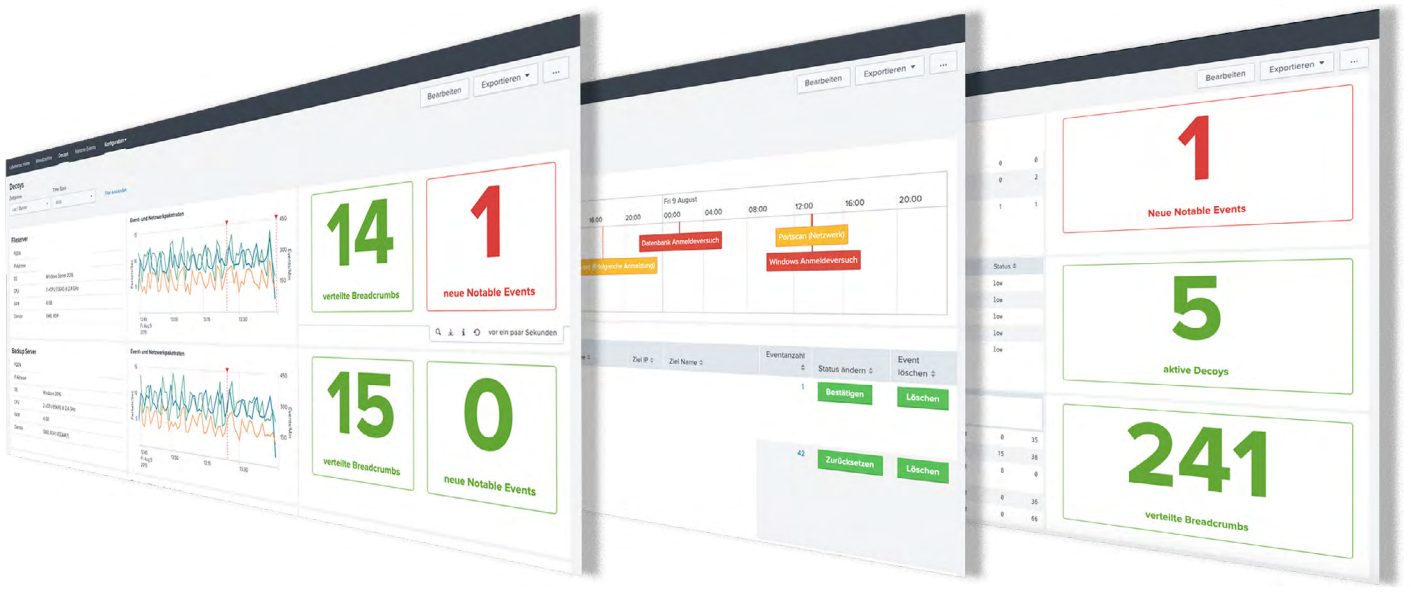



Abbildung: Ansicht der Cybersense Management Konsole mit Anzahl verteilter Breadcrumbs und einem erkannten Angriff

## » CYBERSENSE - ERKENNEN VON EINBRÜCHEN IM **DETAIL**

Neben einer modernen Sicherheitsinfrastruktur zur Angriffsabwehr ist eine Lösung zur schnellstmöglichen Einbruchserkennung unabdingbar. Diese Lösung ist Cybersense angepasst auf die IT-Umgebung legt Cybersense über die unternehmenseigene Softwareverteilung falsche Fährten, sogenannte Breadcrumbs, auf Server und Clients aus. Breadcrumbs sind präparierte Informationen wie etwa Registry-Einträge, die auf dem Client eingespielt werden. Sie werden in einem unauffälligen Muster über das Unternehmensnetz verteilt und locken den Angreifer zu speziell präparierten Servern, den sogenannten Decoys. Die Cybersense Decoys sind eigenständige Server, die für das produktive Unternehmensnetz keine Funktion haben. Diese Unabhängigkeit von Produktivsystemen des Unternehmens macht Cybersense in allen IT-Umgebungen problemlos einsetzbar - auch in KRITIS-Umgebungen wie Krankenhäusern. Die Cybersense Decoys wirken wie Sensoren. Sie sind im normalen, betrieblichen Ablauf nicht auffindbar. Ein Verbindungsaufbau zu einem Decoy kann nur absichtlich von einem Angreifer oder einem Mitarbeiter, abseits seiner normalen Tätigkeit, verursacht werden. Auf seiner Suche nach Informationen nutzt der Angreifer die präparierten Informationen. Cybersense erkennt den verwendeten Breadcrumb und löst Alarm aus. Fehlalarme sind damit ausgeschlossen. Cybersense ist agentenlos - eine Software wird nicht installiert. Das Ausbringen der Breadcrumbs erfolgt über die unternehmenseigene Softwareverteilung mit Hilfe eines Cybersense Installer-Skriptes. Für ein unauffälliges Muster bei der Breadcrumbs-Verteilung sorgt das Cybersense Management. Zusätzlich bietet es detaillierte Informationen über die erkannten Angriffe und den Decoys. Die Alarmierung erfolgt durch das Cybersense Management aus dem Security Operation Center (SOC). Hierfür stehen vielfältige Möglichkeiten zur Verfügung: E-Mails, SMS, Anbindung an vorhandene Systeme (Ticketsystem, SIEM, Network, Monitoring), Security Fabrics bekannter Hersteller.

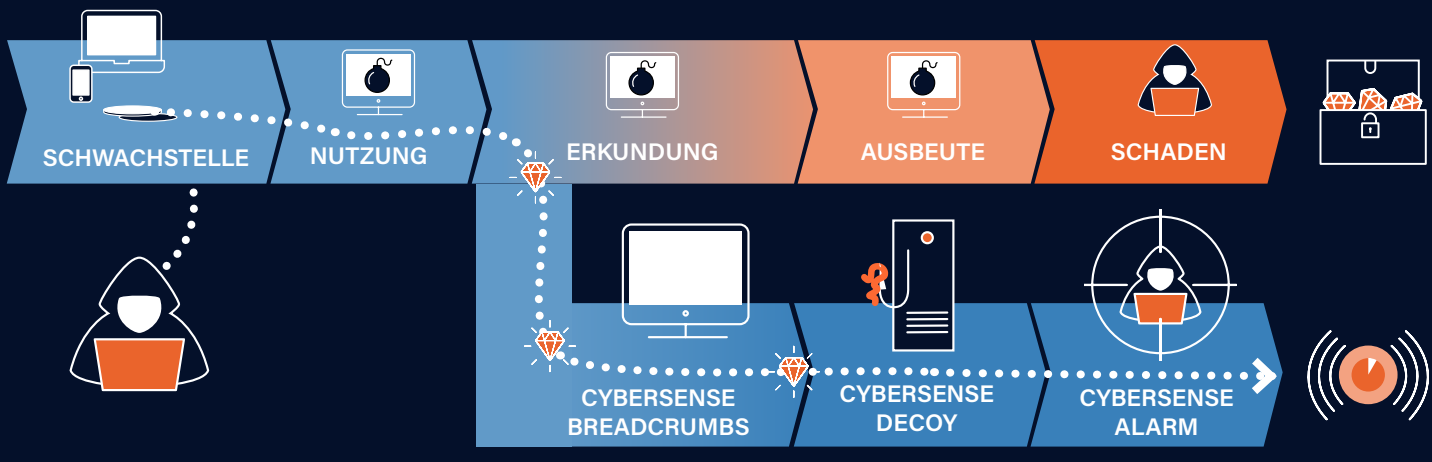



Abbildung: Statt realen Schaden anzurichten, löst der Angreifer mit Cybersense Alarm aus

## » CYBERSENSE - MANAGED SERVICE

Der Cybersense Managed Service unterstützt Sie im Ernstfall: Unsere Experten arbeiten mit Ihren Mitarbeitern zusammen um eine professionelle Einschätzung und Triage durchzuführen.

Auch die Überwachung des laufenden Betriebs und die Pflege der Systeme wird durch die Cybersense GmbH übernommen.

» inklusive regelmäßiger Updates und neuer Breadcrumbs

# »CYBERSENSE - VORTEILE IM ÜBERBLICK

**» FRÜHZEITIGE ERKENNUNG**
Alarmierung in der Erkundungsphase des Angreifers

**» AGENTENLOS**
Keine zusätzliche Software auf Clients oder Servern

**» KOMPLEMENTÄR**
Unabhängig von der vorhandenen Sicherheitsinfrastruktur

**» BETRIEBSSICHER**
Stört vorhandene IT nicht, ideal auch in KRITIS-Umgebungen wie Krankenhäusern

**» KOSTENKONTROLLE**
Einsetzbar auch in Teilbereichen des Unternehmensnetzes

**» KEINE FEHLALARME**
Nur die absichtliche Nutzung von Breadcrumbs löst Alarm aus

## » EIN **ERFAHRENER** PARTNER

**„Unsere Mission ist der Schutz von Unternehmensnetzwerken und sensibler Daten“**

Cybersense beginnt wo konventionelle Sicherheitsmaßnahmen an ihre Grenzen stoßen. Unsere Technologie nutzt proaktiv die schwäche von Angreifern und erkennt Einbrüche einfach und wirksam bevor Schaden entsteht.

Als Experten in verschiedenen Themen rund um die digitale Transformation sind wir Teilnehmer bei der Allianz für Cyber-Sicherheit. Die Allianz für Cyber-Sicherheit ist eine kooperative Plattform vom Bundesamt für Sicherheit in der Informationstechnik (BSI)

Allianz für Cyber-Sicherheit
Teilnehmer

Wir forschen zu IT Security und entwickeln unsere Software an unserem Standort in Dortmund. Dafür führen wir das Vertrauenszeichen von TeleTrusT.

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

## » SIE HABEN **INTERESSE**?

Wenden Sie sich unverbindlich an unseren Vertrieb und vereinbaren Sie ein erstes Gespräch zu Cybersense. Mit den gewonnen Informationen kann anschließend in einem mehrtägigen Kurzprojekt die Wirksamkeit von Cybersense in Ihrer Umgebung eindrucksvoll nachgewiesen werden - auch mittels unabhängiger Penetrationstests. Haben wir Sie überzeugt, ist die Grundlage für die abschließende Inbetriebnahme gelegt.

**» Verantwortlich:** Cybersense GmbH
Martin-Schmeißer-Weg 18 44227 Dortmund
www.cybersense.de

**» Kontakt:**
Telefon: + 49 231 292974 00
E-Mail: info@cybersense.de

»CYBERSENSE
Cybersense GmbH | Martin-Schmeißer-Weg 18 | 44227 Dortmund