»CYBERSENSE

Oberberg Online
MAKING YOUR NET WORK

Angriffserkennung einfach und wirksam

Cybersense Deception entwickelt sich

* für ein „Verfahren für die Verbesserung der Sicherheit in einem elektronischen Kommunikationsnetz“ (Aktenzeichen 10 2021 106 823.1)

Sind Sie sicher...?

Die Ausgangslage

Oberberg Online

»CYBERSENSE

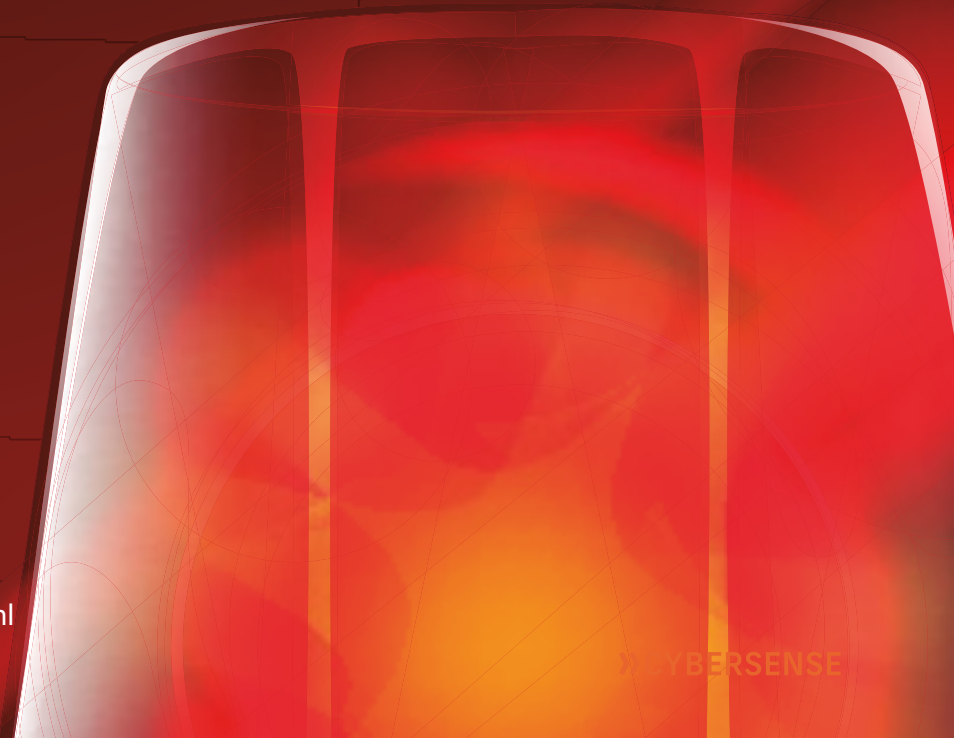
BSI: IT-Bedrohungslage ROT!

→ **Exchange-Lücke Hafnium**

Betroffene Exchange-Server:

weltweit	>100.000
in Deutschland	> mehrere 10.000

... und stündlich mehr!



Quelle: https://www.heise.de/news/Exchange-Luecken-BSI-ruft-IT-Bedrohungslage-rot-aus-5075457.html

Erpresser werden immer aufdringlicher

Oberberg Online

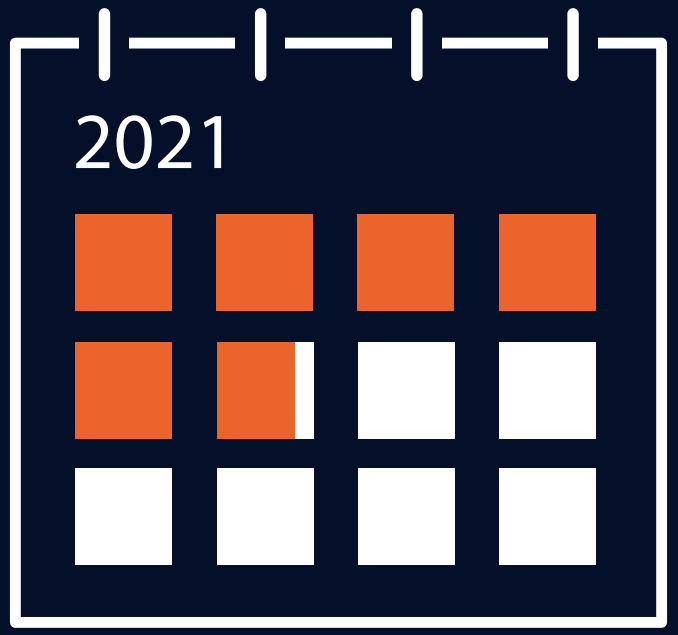
→ **Ransomware REvil**

REvil-Hintermänner üben jetzt noch mehr Druck auf Opfer aus, damit diese Lösegeld zahlen.

Quelle: https://www.heise.de/news/Ransomware-REvil-Erpresser-werden-immer-aufdringlicher-5074106.html

»CYBERSENSE

Frühzeitige Einbruchserkennung



176 Tage

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

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

Dringender Handlungsbedarf!

Neues IT-Sicherheitsgesetz 2.0:
Pflichten und Fristen
für KRITIS-Betreiber und weitere Unternehmen
im besonderen öffentlichen Interesse

Quelle: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/12/it-sig-2-kabinett.html

Oberberg Online

»CYBERSENSE

Dringender Handlungsbedarf!

Für KRITIS-Betreiber u.a.:

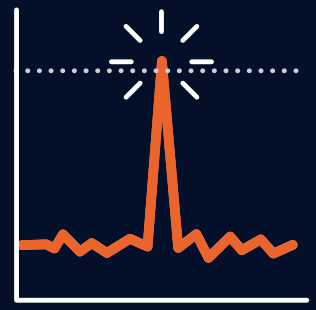
- **Pflicht** zum Einsatz von Systemen zur Angriffserkennung
- **Frist:** 24 Monate nach Inkrafttreten
- **Nachweis:** alle 2 Jahre

https://ag.kritis.info/wp-content/uploads/2021/02/20210125-IT-Sicherheitsgesetz-2.0.pdf – Artikel 1, Nr. 13 b, Änderung §8a

Methoden der Angriffserkennung

Signaturbasiert

Klassisches
IDS/SIEM



Anomalieerkennung

Base Lining mit
Machine Learning

Verhaltensanalyse
(UEBA)

Deception Technology

Decoys und
Breadcrumbs

IT-Sicherheitsgesetz 2.0:

Oberberg Online

sche Muster sowie Verfahren der künstlichen Intelligenz eingesetzt, um Hinweise auf ber-Angriffe zu erhalten. Eine weitere Methode ist es, den störungsfreien Betrieb zu erfassen und dann Abweichungen von diesem Zustand zur Detektion zu verwenden (so genannte Anomaliedetektion).

Die Systeme zur Angriffserkennung sollen die Kommunikationstechnik der Betreiber Kritischer Infrastrukturen möglichst umfassend schützen. Gleichzeitig können Systeme zur Angriffserkennung zum Beispiel im Falle falscher Warnmeldungen auch zu Schäden führen. Gefordert wird daher – entsprechend Absatz 1 – nur ein angemessener Einsatz, dem eine Abwägung der Interessen an einem umfassenden Schutz mit bestehenden Risiken vorgeht.

Unternehmen benötigen für den Einsatz von Systemen zur Angriffserkennung Informationen, die sich als Erkennungsmuster zu Cyber-Angriffen einsetzen lassen. Der Einsatz der Systeme zur Angriffserkennung erfordert, dass die eingesetzten Erkennungsmuster ständig aktuell gehalten werden. Das Bundesamt wird dabei weiterhin, wie in der Vergangenheit geschehen (§ 8b Absatz 2 Nummer 4a), die Betreiber unterstützen. Hierzu wird eigens der

Quelle: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf, Seite 93

So funktioniert Cybersense Deception

Das Wichtigste in Kürze

Oberberg Online

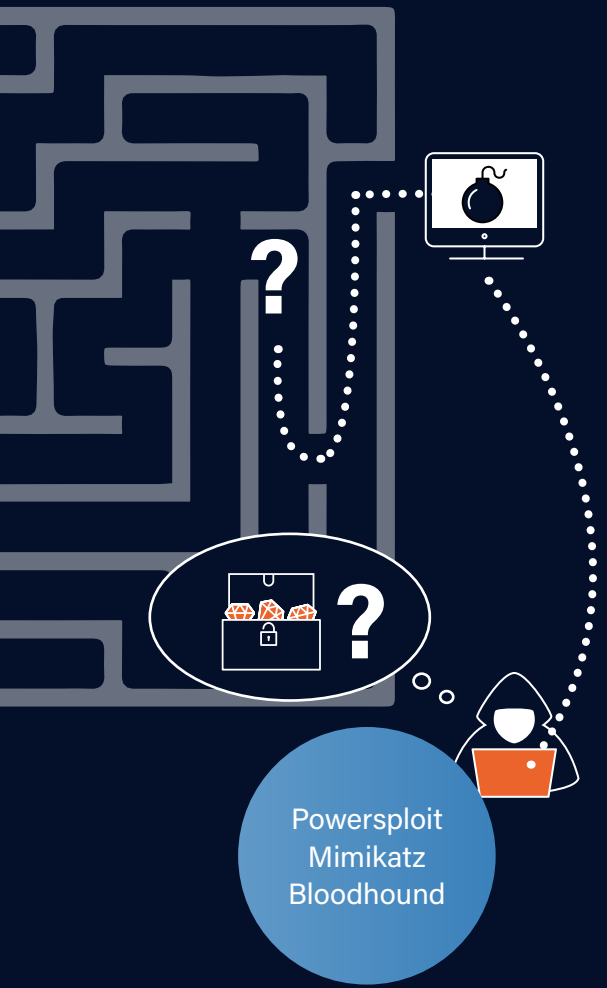
»CYBERSENSE

Deception = Täuschung

Oberberg Online

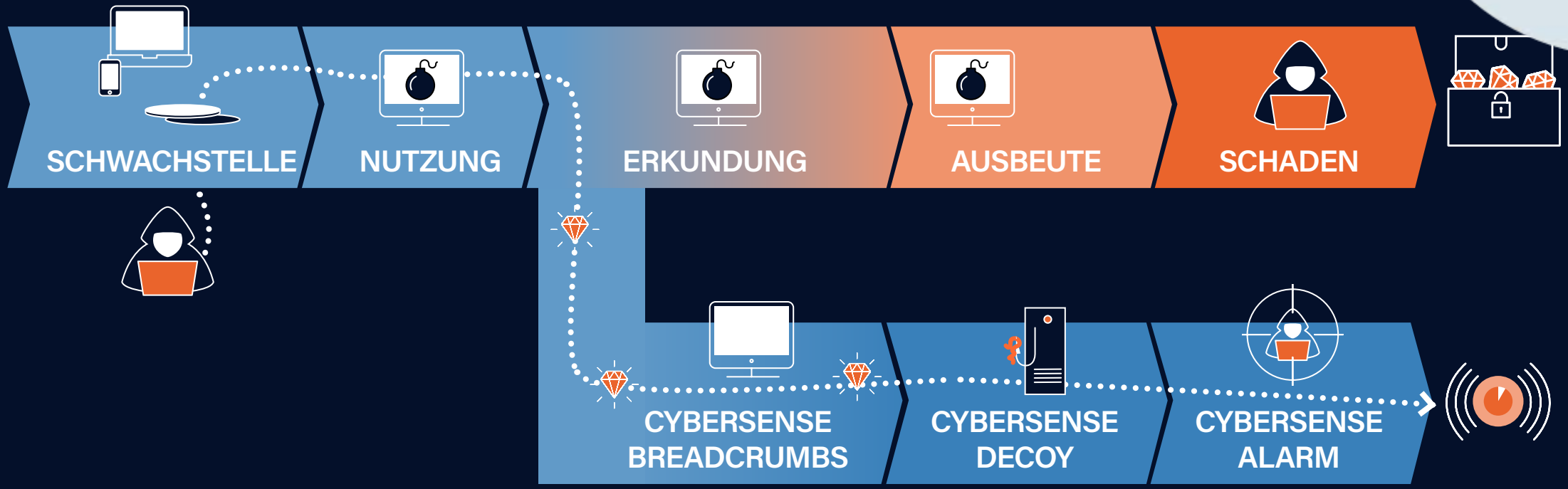
»CYBERSENSE

Cybersense Deception: der Ansatz



- Ein Angreifer muss sich erst einmal orientieren!
- Angreifer nutzen Fehler!
- Ein Angreifer nimmt alles, was er kriegen kann!
- Angreifer benutzen Tools!

Funktionsweise Deception Technology



- Angriffserkennung
- Weiterentwicklung der Honeypot-Technologie
- Falsche Fährten: Breadcrumbs!
- Stolperdrähte: Decoys!

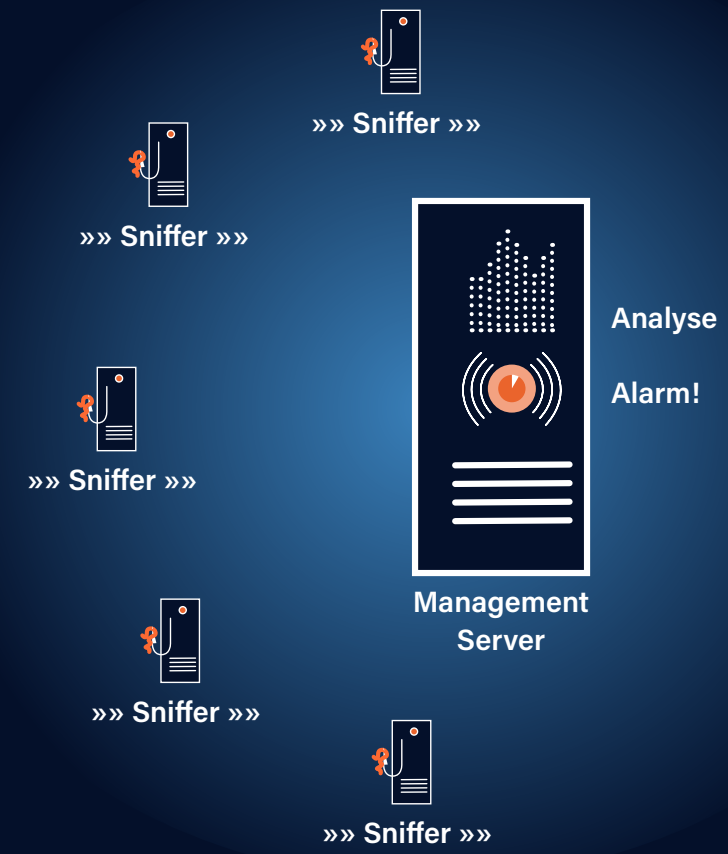
»CYBERSENSE

Decoys

= Lockvogel, Köder

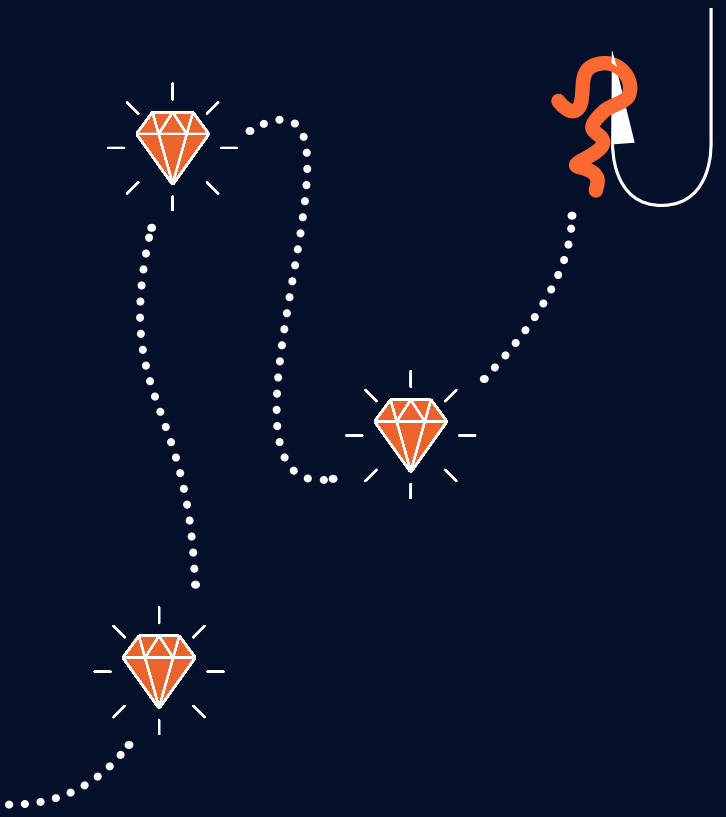
- präparierte Server als Täuschobjekte
- schlagen Alarm bei Verbindung
- bieten vorgetäuschte Dienste
- keine produktiven Aufgaben
- reine Frühwarnsysteme

Decoys



- Echte Server, echte Dienste
- Alle Vorgänge auf den Decoys werden geloggt.
- Jede Applikation ist abbildbar.
- Mitschneiden des gesamten Datenverkehrs
- Server agieren als Schwarm!

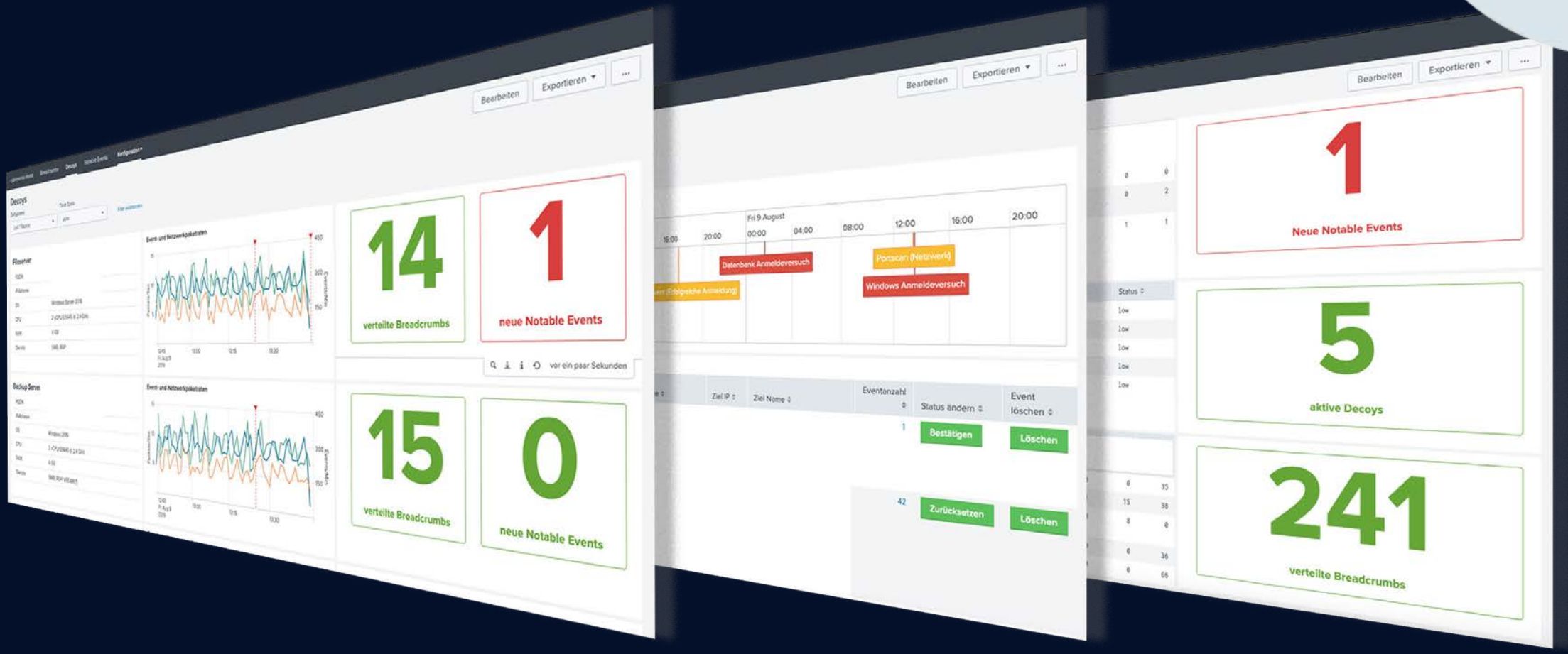
Breadcrumbs / Lures



= Brotkrumen, Info-Leckerli

- unauffällig ausgestreute Informationen auf Clients und anderen Geräten
- lotsen den Angreifer zu den Decoys und weg von der produktiven IT
- individuell und kundenspezifisch

Management System



»CYBERSENSE

Sicherheit mit Cybersense Deception

Die Benefits

Oberberg Online

»CYBERSENSE

Cybersense Deception ist wirksam

Oberberg Online

Frühzeitige Erkennung: Alarm in der Erkundungsphase.

0 % False Positives: Wenige, aber bedeutsame Alarme!

Top Erkennungsraten: Hohe Relevanz gegen aktuelle Bedrohungen.

Betriebssicher: Agentenlos. Läuft störungsfrei neben vorhandener IT.

»CYBERSENSE

Cybersense Deception ist einfach

Oberberg Online

Geringer Aufwand: Automatisiert. Komplementär. Leise.

Kurze Projektlaufzeiten: ca. 2 Tage Aufwand für den Kunden

Kundenindividuell: Deception VMs und Breadcrumbs/Lures

Aussagekräftige Reports zum Sicherheitsstatus und Roll-Out

»CYBERSENSE

Und das Beste: Managed Service!

Oberberg Online

- Unsere Experten arbeiten mit Ihren Mitarbeitern zusammen
- Professionelle Einschätzung und Triage
- Überwachung und Pflege durch Cybersense GmbH
- Stetige Weiterentwicklung

»CYBERSENSE

Cybersense Professional Service

Wir erstellen gemeinsam mit Ihnen Konzepte

- zur Behandlung von Sicherheitsvorfällen
- Festlegung von Eskalationsketten, Verantwortlichkeiten
- Vorauswahl von Incident Respondern und Forensik-Dienstleistern

»CYBERSENSE

Oberberg Online

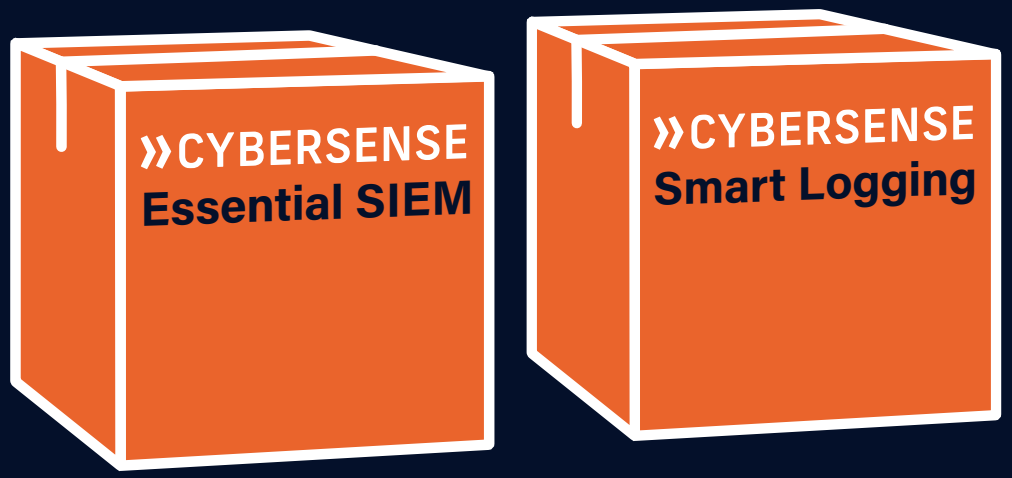
Angriffserkennung einfach und wirksam

Noch eine Minute …

Oberberg Online

»CYBERSENSE

Die nächsten Cybersense-Produkte



Perfekt aufgestellt:

- für die Forderungen von ITSiG 2.0 und neuem BSI Grundschutz
- für den Ernstfall: Forensiker, Incident Responder, LKA
- für Audits: IT-Sicherheit, ISO 27001, Compliance, Revision

Bei Fragen kontaktieren Sie gerne:

OBERBERG-ONLINE INFORMATIONSSYSTEME GMBH

- Dr.-Ottmar-Kohler-Straße 1
  51643 Gummersbach
- **TEL.:** 02261-91550-0
  Fax: 02261-91550-99
- **info@oberberg.net**
  www.oberberg.net

MAKING YOUR NET WORK