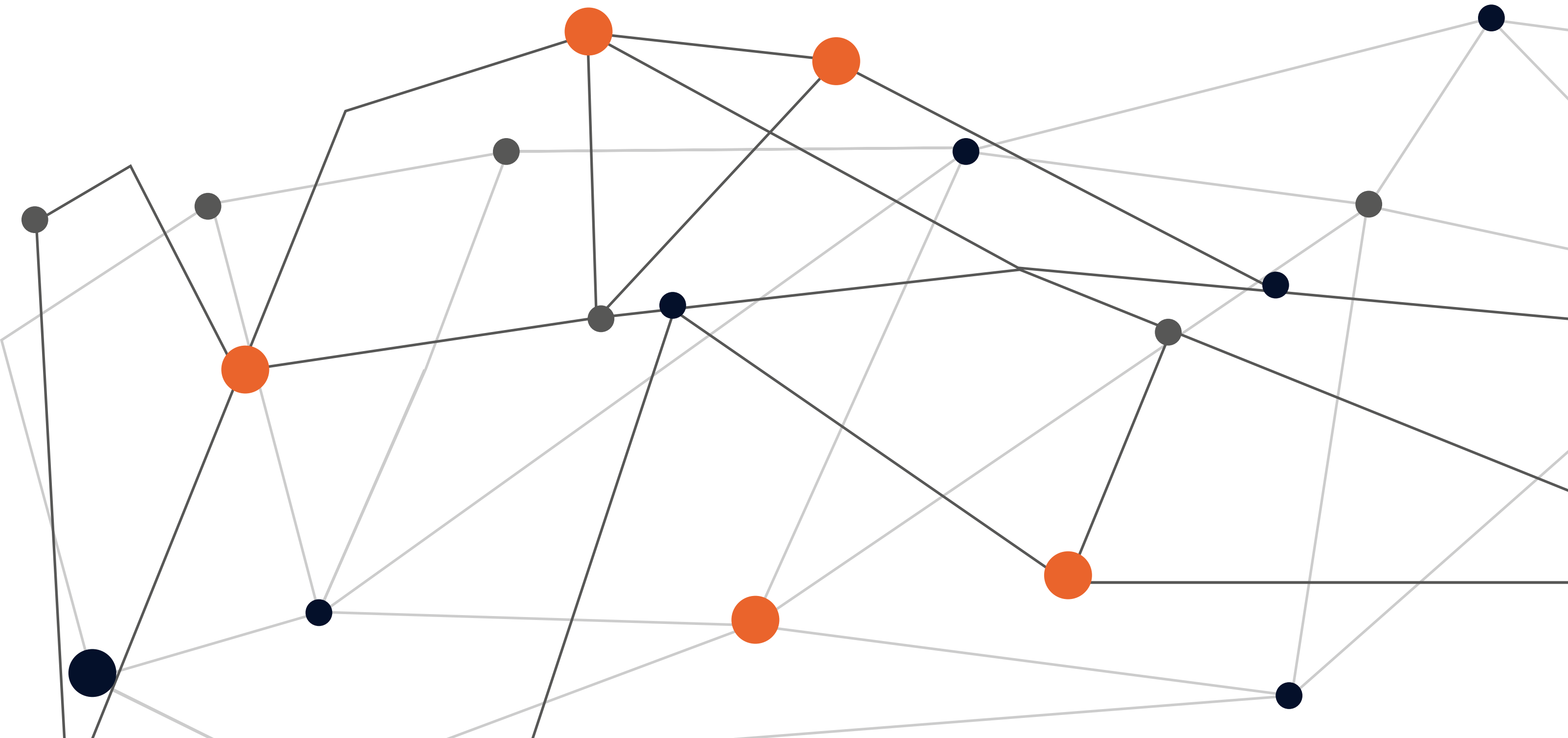
CYBERSENSE

ADVANCED DECEPTION TECHNOLOGY AS A MANAGED SERVICE



CYBERSENSE
ADVANCED DECEPTION TECHNOLOGY AS A MANAGED SERVICE

» INTRUSION DETECTION – EASY AND **EFFECTIVE**

The **CYBERSENSE MANAGED SERVICE** detects intrusions into your corporate network with ease and effectiveness. Cybersense Deception is based on a complementary approach that works independently of existing security systems. During their initial reconnaissance phase, attackers use specially prepared information, which triggers an immediate alert. The attacker has no means of recognizing whether the information gained is genuine and valuable or whether it has been faked by Cybersense Deception.

» DETECTING INTRUSIONS **BEFORE** DAMAGE IS INFLICTED

Damage is inflicted because successful attacks are not detected or detected too late. On average, attackers remain undetected in corporate networks for 6 months. With much creativity and ingenuity, they overcome innovative and intelligent security systems time and again. The number of successful attacks is increasing despite all countermeasures.

68%

of all intrusions are first discovered after weeks or months.

(Source: Verizon, Data Breach Investigations Report 2018, page 6)

176

In Europe, it takes an average of 176 days for an intrusion to be discovered

(Source: FireEye Mandiant, M-Trends Report 2019, Page 6)

» THE **APPROACH** THAT ATTACKERS USE

Most intrusions are not based on highly complex attacks. Rather, attackers use all digital, social or physical means to gain an initial point of entry. This gives the attacker a clear advantage. Once they gain access – usually with low user rights – they attempt to expand their authority in the corporate network and cover their tracks by using relevant attack tools. This is the attacker‘s weak point, which Cybersense Deception cleverly exploits. The attacker is in a completely unknown network and must first explore this environment. Although attackers will proceed very cautiously, ultimately they must use the limited information they have obtained in order to gain more information. Cybersense infiltrates this initial reconnaissance process and provides fake information that triggers an immediate alert.

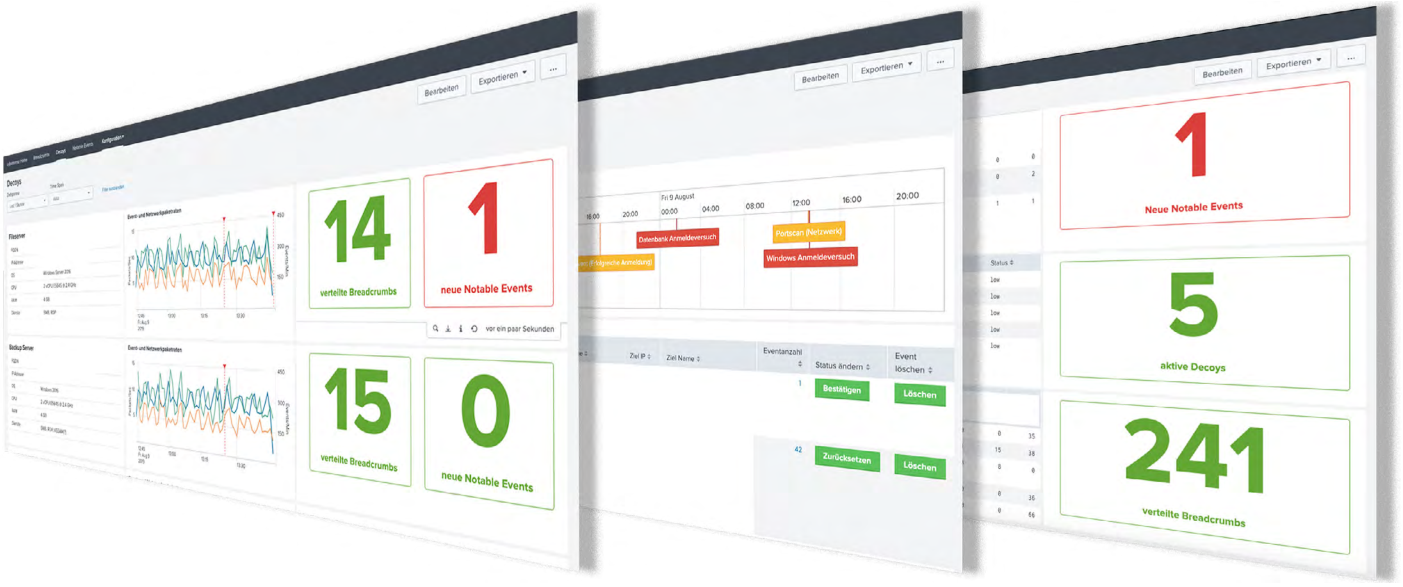


Figure: View of the Cybersense Management Console with number of distributed breadcrumbs and a detected attack.

» CYBERSENSE – DETECTING INTRUSIONS IN **DETAIL**

In addition to modern security infrastructure to defend against attacks, a solution for the fastest possible intrusion detection is essential. This solution is Cybersense, which is adapted to the IT environment and uses the individual company's own software distribution to create false trails, so-called breadcrumbs, on servers and clients. Breadcrumbs are specially prepared information such as registry entries that are imported onto the client. They are distributed in an inconspicuous pattern across the corporate network and lure the attacker to specially prepared servers, the so-called Decoys. The Cybersense Decoys are independent servers that have no function for the productive company network. This independence from the company's productive systems makes Cybersense easy to use across all IT environments – even in KRITIS-environments such as hospitals. The Cybersense Decoys act like sensors. They are not detectable in normal, operational processes. A connection to a Decoy can only be deliberately attempted by an attacker or employees acting outside their normal duties. In their search for information, attackers use the specially prepared information. Cybersense recognizes the breadcrumb used and triggers an alert. False alerts are thereby excluded. Cybersense is agentless - no software is installed. The deployment of breadcrumbs is made via the individual company's own software distribution with the help of a Cybersense installer script. Cybersense Management ensures an inconspicuous pattern in breadcrumb distribution. In addition, it provides detailed information about the detected attacks and Decoys. Alerts are carried out by the Cybersense Management from the Security Operation Centre (SOC). A variety of options are available for this purpose: emails, SMS, connection to existing systems (ticket system, SIEM, network, monitoring), and security fabrics from well-known manufacturers.

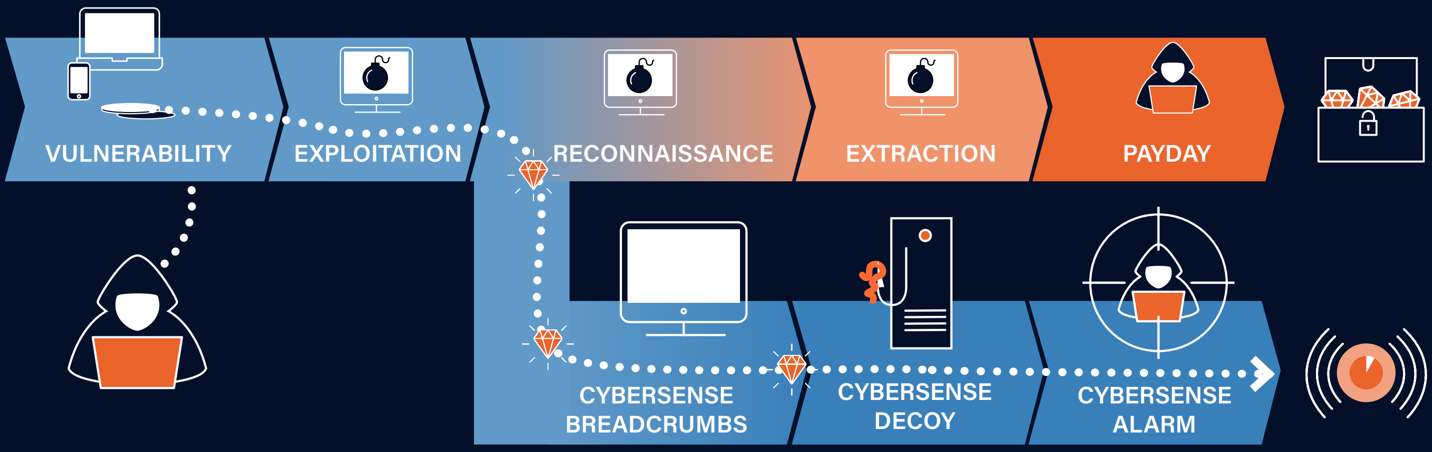


Figure: Instead of inflicting real damage, the attacker triggers an alert with Cybersense

» CYBERSENSE - **MANAGED SERVICE**

The Cybersense Managed Service supports you in the event of an emergency: Our experts work together with your staff to carry out a professional assessment and triage.

Cybersense also takes care of monitoring the ongoing operation and maintenance of your systems.

» Including regular updates and new breadcrumbs

»CYBERSENSE - ADVANTAGES AT A GLANCE

» **EARLY DETECTION**
Alerts during the reconnaissance phase of the attacker

» **AGENTLESS**
No additional software on clients or servers

» **COMPLEMENTARY**
Independent of existing security infrastructure

» **OPERATIONALLY SECURE**
Does not disrupt existing IT, ideal even in KRITIS-enviroments such as hospitals

» **COST CONTROL**
Can also be used in sub-areas of the company network

» **NO FALSE ALERT**
only the intentional use of breadcrumbs triggers alerts

» AN **EXPERIENCED** PARTNER

„Our mission is to protect corporate networks and sensitive data“

Cybersense takes control where conventional security measures reach their limits. Our technology proactively exploits attackers‘ weaknesses and easily and effectively detects intrusions before damage is inflicted.

As experts in various topics related to digital transformation, we are participants in the Alliance for Cyber Security. The Alliance for Cyber Security is a cooperative platform from the Federal Office for Information Security (BSI)

Allianz für Cyber-Sicherheit
Teilnehmer

Cybersense GmbH offers trustworthy IT security solutions made in Germany: We research IT security and develop our software at our location in Dortmund. For this we earned the trust mark of TeleTrusT.

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

» WOULD YOU LIKE TO **LEARN MORE?**

Contact us and arrange an initial non-binding appointment to learn more about the advantages of Cybersense. With the information gained, the effectiveness of Cybersense can then be successfully demonstrated in your environment through a short project lasting several days – including independent penetration tests. Once the decision to implement Cybersense is made, the foundation is already in place for effective launching of the service.

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

» Contact:
Phone: + 49 231 292974 00
E-Mail: info@cybersense.de

»CYBERSENSE

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