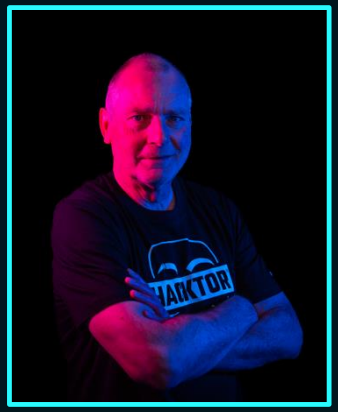
ho.Systeme · 25 Jahre Jubiläum · 11.–12.06.2026

Spielanalyse in Echtzeit

Jeder Angriff. Jeder Spielzug. Jede Reaktion.

Wie Angriffssimulation, Detection und Response technisch ineinandergreifen – Resilient, On-Premises, Made in Germany.

Sascha Hergesell
Presales
sascha.hergesell@enginsight.com

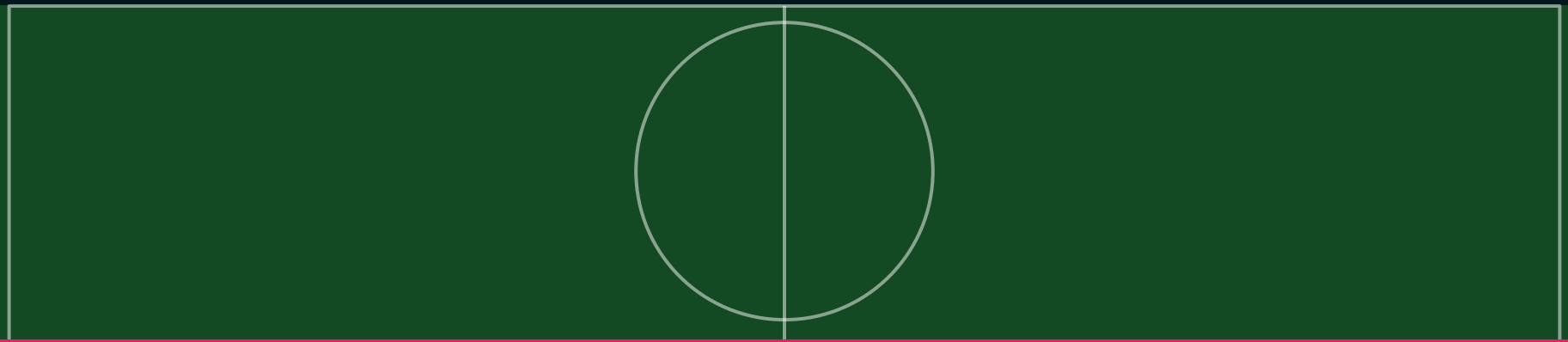


Jürgen Münstermann
Account Executive
juergen.muenstermann@enginsight.com

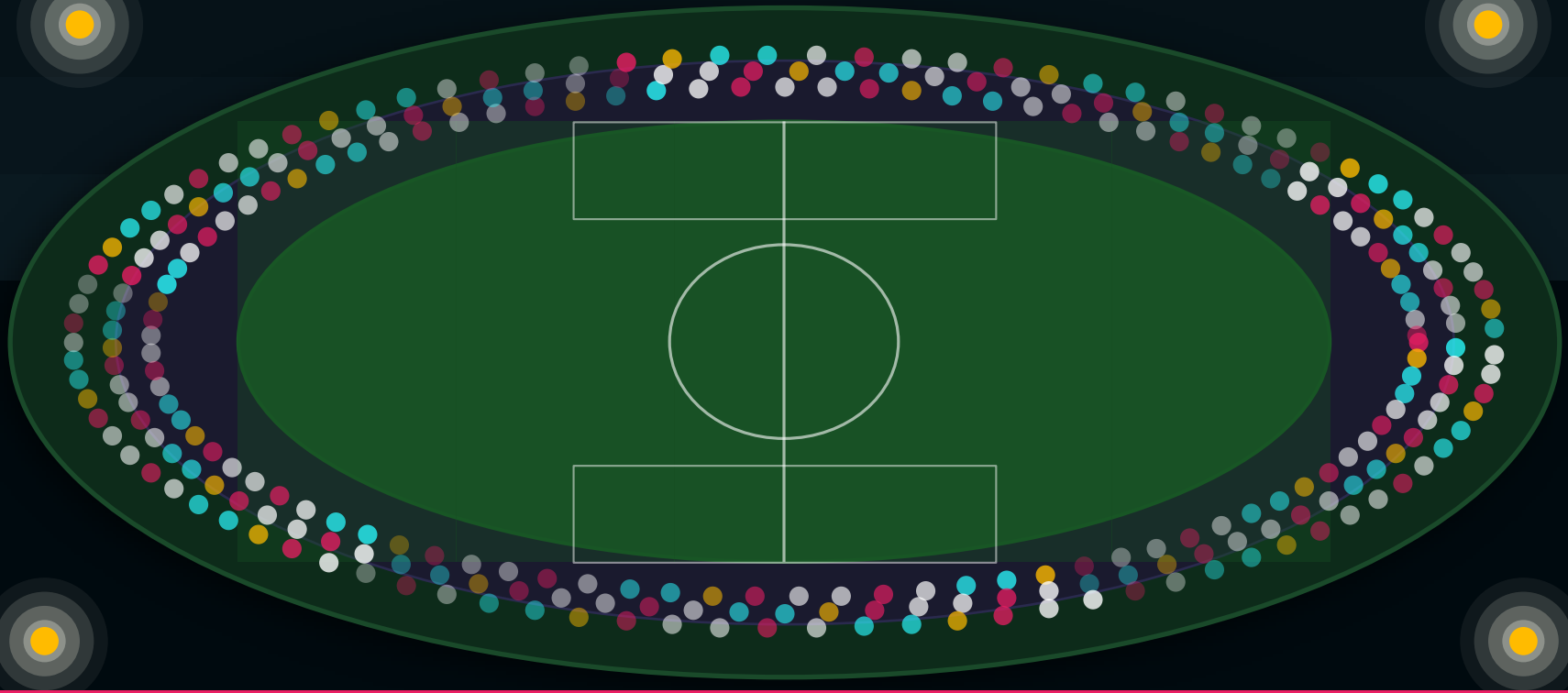
HEIMSPIEL

IT-Sicherheit als Mannschaftssport

ENGINSIGHT



SCHÜCOARENA BIELEFELD · FIFA WM 2026 · MADE IN GERMANY



WILLKOMMEN IM STADION.

SchücoArena Bielefeld · Heimspiel · FIFA WM 2026

DER GEGNER STEHT SCHON AUF DEM PLATZ

Bedrohungslage 2025

22

Minuten

bis eine Schwachstelle ausgenutzt wird

Cloudflare 2024

241

Tage

bis ein Angriff im Durchschnitt erkannt wird

IBM Cost of a Data Breach 2025

289 Mrd.

Euro

Schaden pro Jahr in Deutschland

Bitkom Wirtschaftsschutz 2025

WAS DER ANGREIFER MITBRINGT

Die gegnerische Aufstellung

Steigende Angriffszahlen

Täglich neue Bedrohungen

NIS2 & Compliance-Druck

KRITIS · TISAX · ISO · DORA

GF-Haftung

Bis 10 Mio. € Bußgeld

Zu viele Insellösungen

5–10 Tools ohne Überblick

Fehlende Transparenz

Kein Geräte-Überblick

Sicherheit hinter Firewall

Freie Bewegung nach dem Einbruch

Fehlende Ressourcen

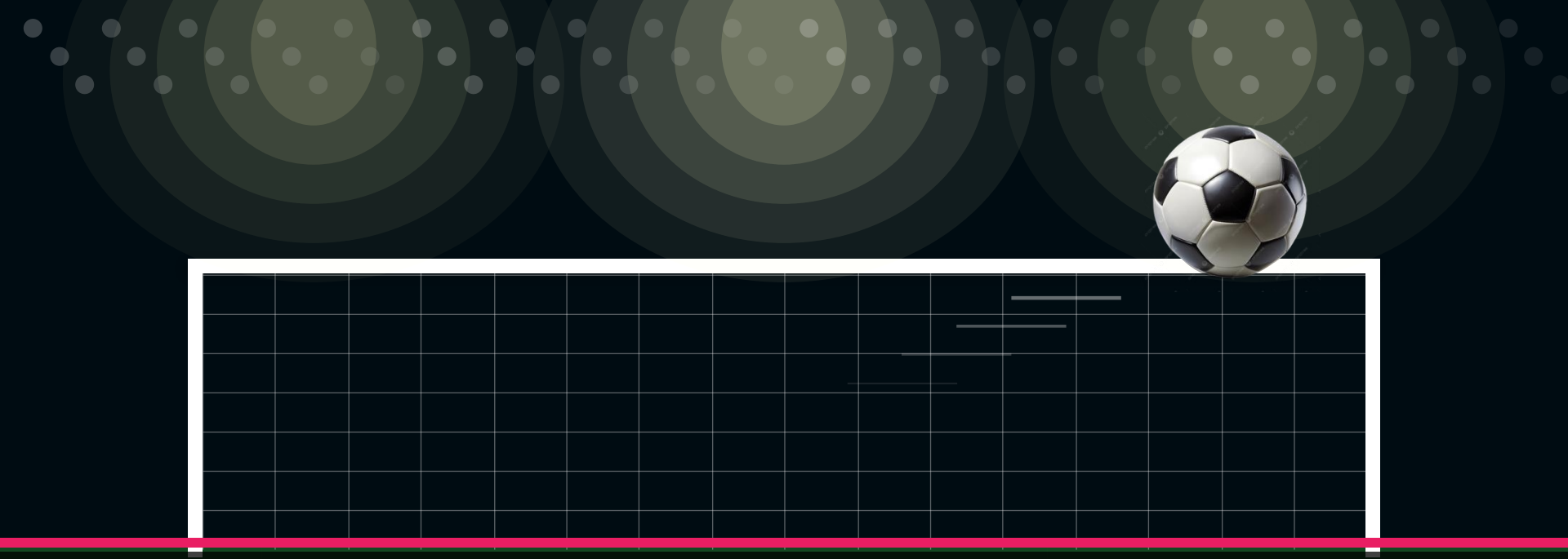
Kein internes SOC

Aufwändiges Reporting

Compliance manuell & teuer

Menschlicher Faktor

Phishing & Social Engineering



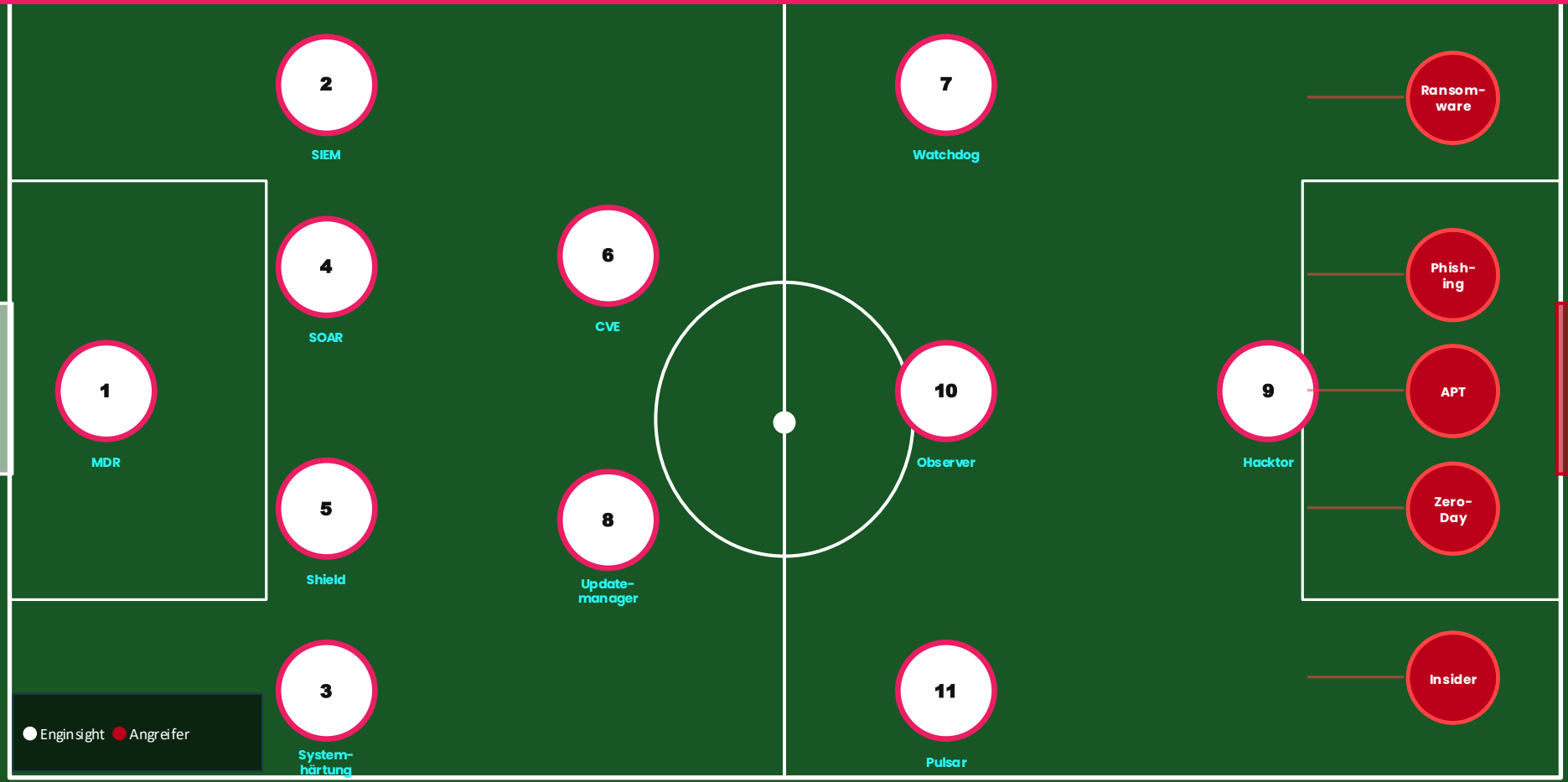
ANPFIFF.

Ihre IT-Infrastruktur braucht ein starkes Team.

ENGINSIGHT · UNITE. SECURE. PROTECT. · 100% MADE IN GERMANY

DIE FORMATION

4 · 2 · 3 · 1 | Heimspiel Allianz Arena



STURMSPITZE: HACKTOR

9

STURMSPITZE

Hacke Dich selbst – bevor es andere tun.

Automatisierter Penetrationstest

Angriff simulieren, bevor Hacker es tun

Schwachstellen-Scan

CVE-Scan & Dienste-Erkennung

Bruteforce-Tests

Passwörter & Zugänge systematisch prüfen

Custom Scripts

Python · Ruby · Bash

Blackbox · Greybox

Alle Testszenarien aus einer Hand

OFFENSIVES MITTELFELD

Nr. 7 · Nr. 10 · Nr. 11 · Sehen, erkennen, melden

7

LINKER AUSSEN

Watchdog

Netzwerk-Scout (agentless)

Kein Gerät bleibt unentdeckt.

- Geräte-Erkennung (Asset Discovery)
- Netzwerk-Inventar
- Agentless Monitoring
- Grundlage für jede Sicherheitsstrategie

10

ZEHNER · SPIELMACHER

Observer

Web- & DNS-Überwachung

Kontrolle über alle digitalen Aussenpfosten.

- SSL/TLS-Zertifikate überwachen
- DNS-Validierung & Änderungen erkennen
- HTTP-Header-Sicherheitscheck
- DSGVO-Bewertung von Webauftritten
- Externe Angriffsfläche im Blick

11

RECHTER AUSSEN

Pulsar Agent

Host-Security & IDS/IPS

Auf jedem System – immer wachsam.

- Intrusion Detection & Prevention (IDS/IPS)
- Datei-Integrität (File Integrity)
- Prozess- & Netzwerküberwachung
- Policy-Manager & Regelwerk
- Direkt auf dem Endgerät – kein Blindspot

DIE DOPPELSECHS: SCHWACHSTELLEN SCHLIESSEN

Nr. 6 & Nr. 8 · Kein bekanntes Einfallstor bleibt offen

6

DEFENSIVES MF

CVE-Management

Schwachstellen erkennen & priorisieren

Kein bekanntes Einfallstor bleibt offen.

- Automatische CVE-Erkennung
- Priorisierung nach CVSS-Score
- Konkrete Handlungsempfehlungen
- Kontinuierliches Monitoring
- Gesamtüberblick der Schwachstellen

8

DEFENSIVES MF

Updatemanager

Automatisches Patching & Härtung

Bekannte Lücken werden automatisch geschlossen.

- Automatische Updates (Auto-Patching)
- Software-Inventar & Versionskontrolle

DIE VIERERKETTE

Nr. 2–5 · Erkennen · Reagieren · Segmentieren · Härten

2

LINKER AV

SIEM

Analyse & Erkennung

- Drittanbieter-Integration (kein Vendor Lock-in)
- Erkennt ungewöhnliches Verhalten
- Zentral-Logging ohne Volumen-Limit

4

IV LINKS

SOAR

Automatische Angriffsbewältigung

- Angriffsbewältigung
- Reaktionspläne & Abläufe (Playbooks)
- Ticketsystem-Anbindung
- KI-gestützte Alarmbewertung

5

IV RECHTS

Shield

Mikro-segmentierung

- Adaptive Netzwerksegmentierung
- Angriffe automatisch stoppen
- Isolierung befallener Netzsegmente
- Minimierung des Angriffsradius

3

RECHTER AV

System-härtung

Konfiguration & Härtung

- automatische Systemhärtung
- Sicherheits-Baselines definieren
- Konfigurationsabweichungen erkennen
- Kontinuierliche Compliance-Prüfung

TORWART: MDR 24/7

TORWART

Der Rückhalt — wenn es wirklich zählt

24 / 7 / 365 Überwachung

Rund um die Uhr – auch wenn alle schlafen

Deutsches Cyber Defence Center

SOC aus Deutschland – DSGVO-konform

Sofortiger Eingriff

Automatisiert oder durch Experten

Volle Transparenz

Keine Blackbox – alle Entscheidungen sichtbar

Hosting-Freiheit

On-Prem · Private Cloud · Public Cloud

DER BETREUERSTAB

Trainer · Physios · Ärzte · Ersatzspieler

TRAINER

Enginsight-Partner

Der Stratege hinter dem Team. Plant die Taktik, kennt den Gegner, führt das Team zu Compliance.

- Channel-First – Partner als Dienstleister
- NIS2-Beratung & ISMS-Aufbau
- Managementtaugliche Sicherheits-Berichte

PHYSIOS

Support-Team 1st & 2nd Level

Halten das Team fit. Schnelle Hilfe bei technischen Problemen, bevor es ernst wird.

- 1st Level: Partner – Erstanlaufstelle
- 2nd Level: Partner – Fehleranalyse
- 3rd Level: Enginsight – Hochkomplex
- Extended Support Paket buchbar

ÄRZTE

Angriffsbewältigung (Incident Response)

Für den Ernstfall. Wenn ein Angreifer durchbricht, sorgen die Ärzte für schnelle Schadensbegrenzung.

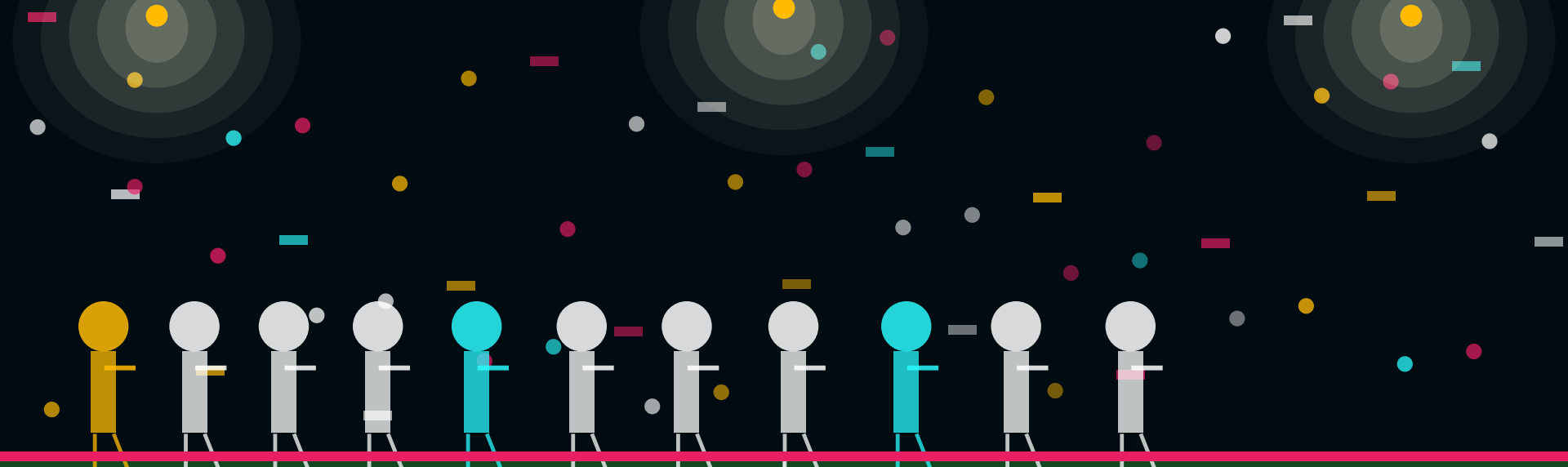
- 24/7 MDR über Cyber Defence Center
- Notfall-Team
- BSI-qualifizierter APT-Response
- Direkter Eingriff auch On-Prem

ERSATZSPIELER

Redundanz & Business Continuity

Der Plan B. Offline-Modus, Backup-Systeme und Redundanz – damit das Spiel weitergeht.

- Offline-/Krisenmodus – voll funktional
- Mandantenfähigkeit
- Hybrides Betriebsmodell: SaaS + On-Prem + Air Gap
- Notfallplan & Forensik-Unterstützung



KEIN EINZELSPIELER GEWINNT EIN SPIEL.

Trainer · Physios · Ärzte · Ersatzspieler · Das komplette Team hinter Ihnen.

DAS SPIELFELD: ARCHITEKTUR

Wo das Spiel stattfindet

SaaS	On-Premises	Private Cloud	Public Cloud
EU-Cloud Enginsight hostet	Ihr Rechenzentrum Volle Datenkontrolle	Ihre eigene Cloud-Infrastruktur	öffentliche Cloud Infrastruktur

KERNKOMPONENTEN

Watchdog Netzwerk-Scout agentless	**Hacktor** Pentest-Flatrate	**Pulsar Agent** Host-Security & IDS/IPS
SIEM Log-Analyse + Machine Learning	**Observer** Web-Monitoring	**SOAR** Auto-Response
Shield Mikrosegmentierung	**MDR** 24/7 SOC	**KI-Plattform** Anomalieerkennung

NIS2: DIE SCHIEDSRICHTERREGELN

Compliance ist kein Freundschaftsspiel

ROTE KARTE
bei Verstoß

10 Mio. €

oder 2 % Jahresumsatz
Wesentliche Einrichtungen (>250 MA oder >50 Mio. € Umsatz)

7 Mio. €

oder 1,4 % Jahresumsatz
Wichtige Einrichtungen (50–249 MA oder 10–50 Mio. € Umsatz)

Geschäftsführer haftet persönlich.

ENGINSIGHT ERFÜLLT ~75 % DER NIS2-ANFORDERUNGEN

- ✓ Regelmäßige Risikoanalyse & Schwachstellenbewertung
- ✓ Geräte-Erkennung, Beschreibung & Software-Inventar
- ✓ Schwachstellen und Sicherheitslücken identifizieren
- ✓ Regelmäßige Penetrationstests der eigenen Infrastruktur
- ✓ Intrusion Detection & Response (IDS/IPS)
- ✓ Log-Management, SIEM & Audit-Trail
- ✓ Angriffsbewältigung (Incident Response)
- ✓ Compliance-Prüfung (BSI · ISO 27001 · TISAX)

STIMMEN AUS DER FANKURVE

Was unsere Kunden sagen

„Einfach und schnell eingeführt. Zuverlässigkeit und direkten Kontakt schätzen wir sehr.“

— Christian Eckerle · Head of IT, HanseYachts AG

„Enginsight rettete unsere TISAX-Zertifizierung.“

— Marcel Pasternak · Schäfer Holding GmbH

„Macht die Software einfach alle glücklich: IT-Admins, Geschäftsführer und Auditoren.“

— Klaus Wilke · GF, MVS Wilke

„Ihr seid das, worauf die Admins bereits seit 15 Jahren warten!“

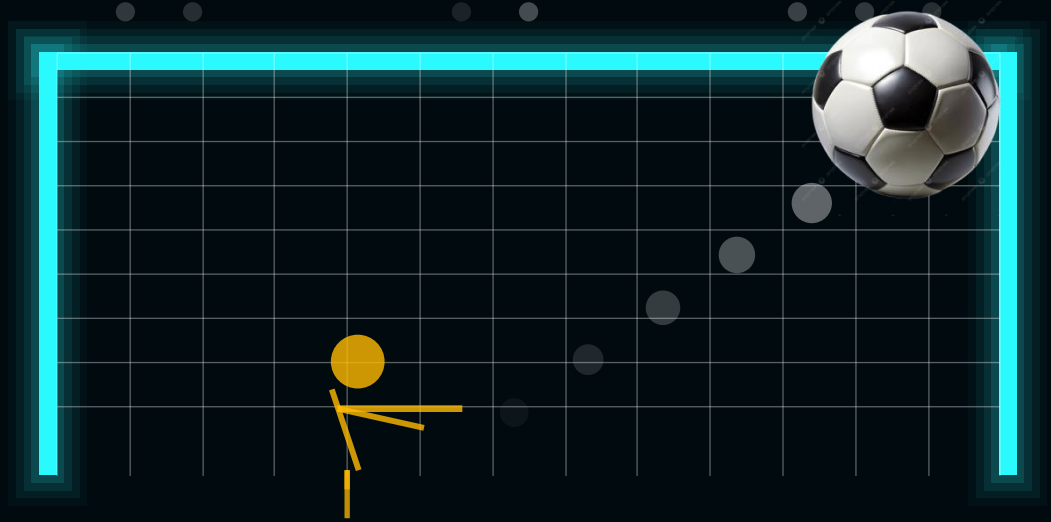
— Heiko Garbe · IT-Manager, SNAP IT GmbH

„Vorher 1–2 Tage pro Woche für Scans. Jetzt nur noch eine Stunde.“

— Chris Trostmann · IT Admin, QSIL GmbH

„Continuous-Überwachung ermöglicht es uns, BaFin-Anforderungen effektiv umzusetzen.“

— Christian Koch · Head of IT, WBG EINHEIT



DER SIEG IST MÖGLICH.

Schützen Sie Ihr Unternehmen — bevor der Angreifer trifft.

ENGINSIGHT · UNITE. SECURE. PROTECT. · 100% MADE IN GERMANY

SCHLUSSPFIFF?

Das Spiel beginnt jetzt erst.

Starten Sie Ihr Heimspiel — kontaktieren Sie uns heute.

enginsight.com | hello@enginsight.com | +49 3641 271 49-39