CYBER SHIELD

//DISCOVER » IMPROVE = PREVAIL

# Cyber Shield

Discover // Improve // Prevail

# Cyber Shield

Die CS Cyber Shield GmbH ist ein in Deutschland ansässiges Unternehmen, das sich auf innovative Cybersicherheits-lösungen und Services spezialisiert hat. Mit modernster Technologie schützt es Unternehmen vor Cyberkriminellen, Espionage, digitalen Bedrohungen und bietet maßgeschneiderte Sicherheits-strategien und Incident Response Services für eine sicherere digitale Zukunft.

# Unsere Mission

**Unsere Mission ist es, Unternehmen, Institutionen und kritische Infrastrukturen vor wachsenden Cyberangriffen zu schützen. Wir setzen uns leidenschaftlich dafür ein, die Sicherheit von geistigem Eigentum, Forschungsergebnissen und Geschäftsgeheimnissen zu gewährleisten sowie die Effizienz in Produktion und Verwaltung aufrecht zu erhalten und zu maximieren.**

# Unsere Prinzipien

## Discover

Unsere Plattformen analysieren Schwachstellen, schützen Daten vor dem Darknet und wehren Cyberbedrohungen wie Ransomware effektiv ab.

## Improve

Wir optimieren Ihre IT-Sicherheit, verbessern bestehende Security Controls und Prozesse oder erweitern sie gezielt – zum Beispiel durch Managed SOC oder Detection-and-Response-Services

## Prevail

Wir schützen IT und OT mit hochwertiger Sicherheitstechnologie, IR und Managed SOC Services. So bleiben Sie vor Cyberangriffen geschützt und können auf das Kerngeschäft fokussiert bleiben

# Unser Team

**Markus Schmitt**
CEO

**Christoph Bernhardt**
CTO

**Fabian Flock**
CCO

**Melinda Varga**
Marketing

**Lea Thießen**
Assistenz

# Unsere Dienstleistungen

- Red Teaming Services: Von der externen Angriffsfläche gestartet, zeigen wir auf wie wir Domain-Admins werden konnten
- Breach- und Attack-Simulation: Testen der Abwehrmechanismen durch fortschrittliche Bedrohungssimulationen.
- KI-gestützte Analysen: Nutzung von KI zur Entdeckung von Sicherheitslücken, sowie Dark-web Monitoring, samt Take Down Service
- Managed SOC in BSI C5 Cloud mit EDR, NDR, MDR, MobileDR, SIEM, SOAR, CSPM, uvm. Inklusive 24x7x365 Monitoring und Alerting auf Sicherheits-vorfälle mittels der marktführenden Technologie
- Cyber Incident Response Services (z.B. als Retainervertrag), Incident Response Trainings

# Discover



**Analyse und Behebung von Schwachstellen**
KI-gestützte Plattformen bieten detaillierte Einblicke in Angriffsflächen und ermöglichen die Identifikation und Behebung von Sicherheitslücken in Echtzeit.

**Dark Web-Überwachung und Schutz sensibler Daten**
Die Überwachung von Aktivitäten im Darknet hilft dabei, potenzielle Bedrohungen frühzeitig zu erkennen und Datenmissbrauch zu verhindern.

**Risikomanagement bei Drittanbietern**
Third Party Risk Management (TPRM) bewertet und minimiert Risiken, die durch die Zusammenarbeit mit Drittanbietern entstehen können.

**Markenschutz und Betrugsbekämpfung**
Innovative Takedown-Services schützen Marken vor Phishing, Identitätsdiebstahl und betrügerischen Domains und tragen zur Sicherung der digitalen Integrität bei.

**Proaktive Abwehr gegen Cyberbedrohungen**
Lösungen wie Cyble stärken die Sicherheit gegenüber Ransomware, Account-Übernahmen und anderen Bedrohungen durch kontinuierliche Überwachung und fortschrittliche Technologien.

# Improve



**Automatisierte Penetrationstests**

- Kosteneffiziente, kontinuierliche Schwachstellenanalyse zur Risikominimierung / Erfüllung von KRITIS / DORA
- Ergänzung manueller Tests für tiefgehende Sicherheitsanalysen.

**Breach and Attack Simulation (BAS)**

- Umfassende Validierung der vorhandenen Security Controls (Firewalls, EPP/EDR, Email Security, SIEM, etc.)
- Kontinuierliche Optimierung der Cybersecurityprozesse (Incident Response) durch realistische Angriffssimulationen.

**Kontinuierliches Bedrohungsmanagement (CTEM)**

- Sicherheitsdaten und Bedrohungsinformationen verknüpfen, um gezielte Maßnahmen zu ermöglichen.
- Ständige Verbesserung der Sicherheitsstrategie zur Risikoreduzierung.

**Optimierung der Sicherheitsstrategie**

- Priorisierung von Bedrohungen und Schwachstellen durch umfassende Analysen.
- Erhöhung der Effizienz und Skalierbarkeit durch automatisierte Tests.

**Effektive Kombination aus Tests und Monitoring**

- Realistische Simulationen und automatisierte Scans liefern kontinuierlich wertvolle Erkenntnisse.
- Verbesserung der Sicherheitslage durch präzise Identifikation und Behebung von Schwachstellen.

# Prevail



**IT-Schutz für KMUs**

- Rund-um-die-Uhr Überwachung und automatisierte Bedrohungsabwehr mit XDR-Lösung.
- Effiziente Sicherheitsprozesse durch SOAR-Funktionen, speziell für kleine Unternehmen.

**Umfassende XDR-Lösung**

- Integration von CTI, SOAR, Honeypots und proprietärer KI für Echtzeiterkennung.
- Minimale menschliche Interaktion für proaktiven Schutz gegen fortschrittliche Bedrohungen.

**Phish-Sichere MFA**

- Schutz vor Anmeldedaten-Diebstahl und passwortbasierten Angriffen.
- Vereinfachte und kosteneffiziente Lösung für kompromisslose Sicherheit.

**Revolutionäre Identitätssicherheit**

- Schutz sensibler Ressourcen mit agenten- und proxyfreier Architektur.
- KI-gestützte Risikoanalyse und Echtzeit-Bedrohungsblockierung für moderne IT-Umgebungen.

# Angebote passend zur Unternehmensgröße

## Große Unternehmen

- **Ganzheitliches Bedrohungsmanagement (CTEM**): Früherkennung relevanter Bedrohungen, Proaktive Risikominderung, Priorisierung vorrangiger Maßnahmen, kontinuierliche Verbesserung der Sicherheit
- **Mikrosegmentierung:** Mikrosegmentierung endlich richtig umgesetzt, führt dazu, dass sich Angreifer nicht mehr durch Ihr Netzwerk bewegen, oder es umfassend verschlüssen oder zu einem Bot-Net machen können
- **Managed SOC-Dienste:** Rund-um-die-Uhr-Überwachung und Bedrohungsmanagement durch ein spezialisiertes Security Operations Center.
- **Breach and Attack Simulation (BAS):** Realistische Angriffssimulationen zur Verbesserung von SIEM, Firewalls, EDR-Tools, Email-Security, DLP und mehr – samt Integrationen zur vereinfachten Verbesserung
- **Red Team Services:** Nutzung von hochwertigen Darkweb Quellen, Social Engineering, Ausnutzung von Schwachstellen in der externen Angriffsfläche (webservices), um per Lateral Movement zu Ordnern, Dateien, Server vorzudringen, Exfiltration von Daten, Übernahme priviliegerter Accounts oder Simulation von Verschlüsselung; Ergebnis-Analyse

## KMUs und Startups

- **Cynet MDR:** Budgetfreundliche XDR-Lösung mit 24/7-Überwachung und automatisierter Bedrohungsabwehr.
- **Cyber Incident Response Service:** Vertragliche Zusicherung von unserem Incident Response Service, falls Ihr Unternehmen einem Cyberangriff zu Opfer gefallen ist; Definierte deutsche Ansprechpartner, garantiertes höchstmaß an Effizienz; kontinuierliche Verbesserung inkl.
- **Breach and Attack Simulation (BAS)**: Für Startups und kleinere Unternehmen, um bestehende Sicherheitsmaßnahmen zu überprüfen und zu verbessern.
- **Silverfort MFA**: Revolutioniert Identitätssicherheit in Local AD und Hybrid Umgebungen, Identity Detection and Response, MFA-Anything
- **AuthN by IDEE**: Effektive und preiswerte MFA-Lösung zum Schutz der digitalen Identitäten Ihrer Mitarbeiter im Unternehmen, Senkung von Support Anfragen; Phishing Schutz

# Unsere Partner

Allianz für Cyber-Sicherheit
Teilnehmer

ZERO Networks

In Kooperation mit
CYBERsicher NOTFALLHILFE

SILVERFORT

IONIX

PICUS

cynet

IDEE

CYBLE®

TEHTRIS
FACE THE UNPREDICTABLE

# Cyber Shield

Discover // Improve // Prevail


CS Cyber Shield GmbH

**Markus Schmitt, Geschäftsführer**
+49 174 260 1741; msc@cyber-shield.org

**Christoph Bernhardt, Chief Technology Officer**
+ 151 5488 9241; cbe@cyber-shield.org

Anschrift:
Zum Wartturm 5,
63571 Gelnhausen,
Deutschland



HRB 99474
Amtsgericht Hanau;
Sitz der Gesellschaft: Gelnhausen;
Geschäftsführer: Markus Schmitt

Steuernummer: 019 230 40030
USt-IdNr.: DE363562591