CYFIDELITY

Excellence in Cyber-Resilience

Ein Unternehmen der Oetker-Gruppe

Über uns

CYFIDELITY

Die Cyfidelity ist ein spezialisiertes IT-Security- und Compliance-Beratungsunternehmen und Teil der Oetker-Gruppe.

Unser Team aus rund 25 erfahrenen Sicherheitsexperten unterstützt mittelständische Unternehmen und Konzerne – insbesondere in regulierten und industriellen Umfeldern – bei der gezielten Stärkung ihrer technischen und organisatorischen Resilienz.

Wir verbinden strategische Beratung mit fundierter technischer Expertise in der Wirksamkeitsprüfung von Sicherheitsmaßnahmen sowie der Erkennung und Eindämmung komplexer Cyberangriffe, einschließlich operativ erprobter 24/7 Incident-Response-Kompetenz.

Unser Ansatz

CYFIDELITY

Cyfidelity steht für den strukturierten und wirksamen Aufbau strategischer, taktischer und operativer Cyber-Resilienz.

Unser Ansatz verbindet drei ineinandergreifende Kompetenzbereiche:

Offensive Security Services

Realistische Sicherheitsprüfungen und Angriffssimulationen

Defense Operations & Preventive Engagements

Stärkung der operativer Verteidigungsfähigkeit

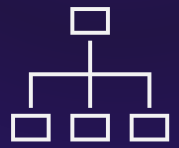
Resilience & Compliance Advisory

Stärkung der organisatorischen Verteidigungsfähigkeit

Gemeinsam etablieren sie Cyber-Resilienz als unternehmerische Fähigkeit – geprägt von technischer Exzellenz und klarem Qualitätsanspruch.

Offensive Security Services

CYFIDELITY



Offensive Sicherheit beginnt mit einem realistischen Verständnis der eigenen Angriffsfläche. Wir simulieren gezielte Angriffsszenarien, um technische Schwachstellen sichtbar zu machen und die Wirksamkeit bestehender Sicherheitsmaßnahmen objektiv zu überprüfen.

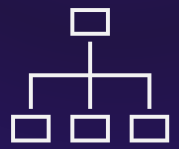
Schwerpunkte:

- Red Teaming
- Purple Teaming
- Penetration Testing
- Security Audits
- OT-Risk Assessments

Dabei identifizieren wir nicht nur technische Schwachstellen, sondern bewerten deren reale Ausnutzbarkeit und geschäftliche Relevanz. So schaffen wir eine belastbare Grundlage für fundierte Priorisierung und wirksame Maßnahmen.

Offensive Security Services

CYFIDELITY



Red Teaming

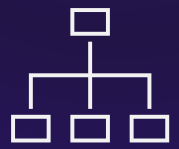
Realitätsnahe, unabhängige Prüfung der Widerstandsfähigkeit unter operativen Angriffsbedingungen.

- Simulation komplexer, zielgerichteter Angriffsszenarien
- Überprüfung von Detection-, Response- und Eskalationsprozessen
- Identifikation strategischer Schwachstellen über technische Einzelfehler hinaus
- Bewertung organisatorischer Reaktionsfähigkeit

Unsere Engagements basieren auf realitätsnahen Angriffsmustern, klar definierten Zielsetzungen und strukturierter Ergebnisaufbereitung mit priorisierten Handlungsempfehlungen.

Offensive Security Services

CYFIDELITY



Purple Teaming

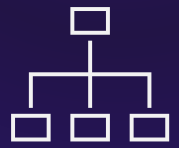
Kollaborativer Ansatz zur gezielten Weiterentwicklung von Detection- und Response-Fähigkeiten.

- Enge Zusammenarbeit mit internen Blue Teams
- Gemeinsame Analyse realer Angriffspfade
- Optimierung von Erkennungsmechanismen (Use Cases, Playbooks)
- Verkürzung von Reaktionszeiten und Verbesserung der Wirksamkeit

Praxisnahe Szenarien und eine strukturierte Aufbereitung bilden die Basis für unsere präzisen Analysen und priorisierten Pläne zur Sicherheitsoptimierung.

Offensive Security Services

CYFIDELITY



Penetration Testing

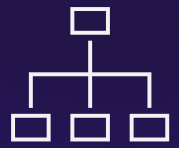
Gezielte Identifikation und Ausnutzung technischer Schwachstellen in IT-Systemen.

- Methodische Prüfung von Applikationen, APIs,Netzwerken und Cloud-Instanzen
- Aktive Verifikation von Sicherheitslücken und Patch-Ständen
- Standardisiertes Vorgehen bspw. nach OWASP und BSI-Leitfäden
- Fokus auf technische Fehlkonfigurationen und Einzelsysteme

Unsere Tests liefern präzise Analysen und priorisierte Maßnahmen zur effektiven Härtung Ihrer technischen Infrastruktur.

Offensive Security Services

CYFIDELITY



Security Audit

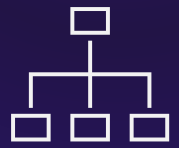
Strukturierte Prüfung von Konfigurationen und Compliance-Vorgaben gegen Best Practices.

- AD Security Check: Analyse der Identitätsverwaltung auf Fehlkonfigurationen, Berechtigungsrisiken und die korrekte Umsetzung von Tiering-Modellen.
- M365 Security Check: Audit der Cloud-Konfiguration mit Fokus auf Identitätsschutz (MFA/CAP), sicheren Datenzugriff und lückenlose Protokollierung.
- Client Security Check: Bewertung des Härtungsgrads und Patch-Stands der Endgeräte auf Basis von CIS-Benchmarks und Security Baselines.
- Netzwerksegmentierung: Überprüfung der Zonentrennung und Firewall-Regelwerke zur Kontrolle interner Verkehrsflüsse nach Industriestandards.

Unsere Audits liefern eine präzise Bestandsaufnahme Ihres Sicherheitsniveaus sowie konkrete Handlungsempfehlungen zur Erreichung höchster Compliance-Standards.

Offensive Security Services

CYFIDELITY



OT-Risk Assessment

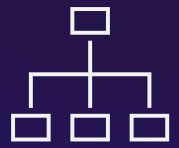
Strukturierte Risikoanalyse für industrielle Steuerungs- und Automatisierungssysteme (IACS).

- Asset-Identifikation und Modellierung von Zonen & Conduits
- Bedrohungsanalyse spezifisch für Produktions- und Prozessumgebungen
- Gap-Analyse gegen Security Level (SL) Anforderungen der IEC 62443
- Bewertung der Resilienz von Fernwartung und Netzwerksegmentierung

Unsere Assessments liefern eine belastbare Entscheidungsgrundlage zur Absicherung Ihrer Anlagenverfügbarkeit und zur Erfüllung regulatorischer Anforderungen.

Defense Operations & Preventive Engagements

CYFIDELITY



Operative Sicherheit entscheidet sich nicht im Konzept, sondern im Ernstfall.

Wir unterstützen unsere Kunden beim Aufbau belastbarer Reaktions- und Verteidigungsstrukturen – vor, während und nach Sicherheitsvorfällen.

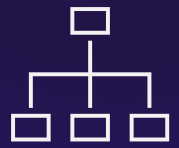
Schwerpunkte:

- Digital Forensics & Incident Response (DFIR)
- 24/7 Einsatzbereitschaft
- Incident Response Preparation
- Krisenstabs- und Notfall-Übungen
- Detection Engineering & Response-Optimierung

Ziel ist es, bei einem Cyberangriff schnell, strukturiert und wirksam handlungsfähig zu sein.

Defense Operations & Preventive Engagements

CYFIDELITY



Vorbereitung & Organisation

- Strukturierte Notfallplanung mit klar definierten Entscheidungswegen
- Entwicklung belastbarer Incident-Response-Playbooks
- Aufbau einer handlungsfähigen Krisenorganisation
- Praxisnahe Krisenstabs- und Notfall-Übungen

Reaktion im Vorfall

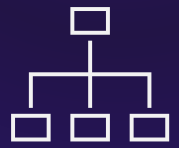
- 24/7 Einsatzbereitschaft
- Incident Response einschließlich Eindämmung und Digital Forensics (DFIR)
- Abstimmung interner und externer Entscheidungsträger

Stabilisierung & Weiterentwicklung

- Wiederherstellung der operativen Handlungsfähigkeit
- Strukturierte Aufarbeitung und Ableitung von Verbesserungsmaßnahmen

Resilience & Compliance Advisory

CYFIDELITY



Nachhaltige Cyber- Resilienz erfordert die abgestimmte Steuerung strategischer, taktischer und operativer Ebenen.

Schwerpunkte:

- Aufbau und Weiterentwicklung von Informationssicherheits-Managementsystemen (z. B. ISO 27001, BSI IT-Grundschutz)
- Umsetzung regulatorischer Anforderungen (z. B. NIS2, KRITIS, B3S, DORA, TISAX)
- Aufbau und Weiterentwicklung von Business-Continuity-Managementsystemen (ISO 22301, BSI 200-4)
- Beratung auf Führungsebene im Security Management (z. B. CISO as a Service)
- Cyber Resilience Management (CRMS) – unsere risikobasierte Methodik zur integrierten Steuerung von Cyber- Resilienz über alle Ebenen hinweg

Wir verbinden fachliche Expertise, internationale Projekterfahrung und fundierte Methodik in der strukturierten Umsetzung komplexer Anforderungen.

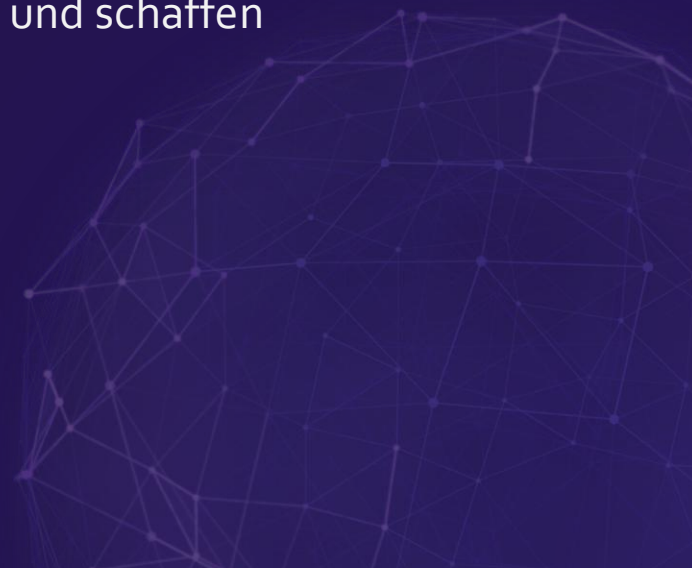
Unser Anspruch

CYFIDELITY

Wir denken Cyber Resilienz ganzheitlich.

Mit technischer Expertise und unabhängiger Beratung schaffen wir Transparenz über reale Risiken und unterstützen dabei, die richtigen Schwerpunkte zu setzen – geprägt von einem klaren Qualitätsanspruch und konsequenter Ausrichtung auf Wirksamkeit.

Als verlässlicher Partner begleiten wir unsere Kunden auf dem Weg zu mehr Resilienz und schaffen Strukturen, die im Alltag verlässlich funktionieren und im Ernstfall standhalten.



Kontakt

CYFIDELITY

Gerne besprechen wir mit Ihnen die nächsten Schritte ihrer Cyber-Resilienz.

Stefan Hebler
Mobil: 0176 6946994
E-Mail: stefan.hebler@cyfidelity.com

Cyfidelity Security Services GmbH
Bechterdisser Str. 10
33719 Bielefeld

24/7 Cyber Emergency Hotline:
0800 3 666 404
Germany - Austria - Switzerland