# Lieferanten-Due-Diligence & Sicherheitsvertrauen

Wie Cyber Crucible Fragebögen zum Anbieterrisiko für Unternehmen und Finanzinstitute beantwortet — was gehalten wird und was nicht, wie regulatorische Pflichten unterstützt werden, wie KI gesteuert wird, welche Servicelevels gelten und wie die Architektur Drittparteirisiken reduziert. Klar und ehrlich dargestellt.

# Verfügt Cyber Crucible über einen SOC-2-Bericht?

**Kurze Antwort:** Nein. Cyber Crucible verfügt derzeit über kein SOC-2-Attest und weist ausdrücklich darauf hin, anstatt etwas anderes anzudeuten. Der Grund ist architektonischer Natur: Cyber Crucible ist ein lokal ausgeführtes Softwareprodukt und kein Cloud-Verwahrer von Kundendaten. Daher lässt sich das SOC-2-Modell für Dienstleistungsorganisationen – das bescheinigt, wie ein Anbieter *Ihre* Daten auf seinen eigenen Systemen speichert, verarbeitet und überträgt – nicht sauber darauf übertragen.

# Warum die meisten Kunden bisher keinen SOC-2-Bericht verlangt haben

SOC 2 bescheinigt die Kontrollen einer Dienstleistungsorganisation, die Kundendaten verwahrt. Das Design von Cyber Crucible hebt diese Grundvoraussetzung auf:

- Bedrohungserkennung und -reaktion erfolgen auf dem Endpunkt, auf Kernel-Ebene, auf dem eigenen Gerät des Kunden.
- Kundendateien, Anmeldeinformationen, Verschlüsselungsschlüssel und Sitzungstoken werden von Cyber Crucible niemals erfasst, übertragen oder gespeichert.
- Die Plattform kann vollständig vor Ort (on-premises) oder abgeschottet (air-gapped) innerhalb der eigenen Infrastruktur des Kunden bereitgestellt werden.

Da die risikoreichsten Datenkategorien niemals in den Besitz von Cyber Crucible gelangen, wird ein großer Teil der Angriffsfläche im Lieferantenrisiko, die ein SOC-2-Bericht adressieren soll, bereits durch das Design beseitigt und nicht nur kontrolliert.

# Was an dessen Stelle tritt

Für Prüfer, die anhand eines Fragebogens arbeiten, stellt Cyber Crucible ein vorbereitetes Sicherheitspaket für Anbieter bereit, das die zugrunde liegenden Kontrollnachweise direkt liefert und die Kontrollen von Cyber Crucible den SOC-2-Trust-Service-Kriterien sowie dem NIST Cybersecurity Framework zuordnet, sodass ein Prüfer einen Standardfragebogen darauf basierend ausfüllen kann. Das Paket ist unter einer gegenseitigen Vertraulichkeitsvereinbarung (NDA) über **dpo@cybercrucible.com** erhältlich.

Die Roadmap für Zusicherungen (Assurance) wird laufend im Hinblick auf die Kundenbedürfnisse evaluiert; diese Seite wird aktualisiert, sollte sich diese Position ändern.

# Ist Cyber Crucible nach ISO 27001, PCI-DSS, CMMC oder FedRAMP zertifiziert?

**Kurze Antwort:** Nein. Cyber Crucible hat keine ISO/IEC 27001-, PCI-DSS-, HIPAA-, CMMC- oder FedRAMP-Zertifizierung bzw. -Autorisierung erlangt und erhebt auch keinen entsprechenden Anspruch. Dies wird ausdrücklich klargestellt, da die Behauptung einer Zertifizierung, die ein Anbieter nicht besitzt, genau die Art von Widerspruch darstellt, die das Vertrauen in eine Sorgfaltsprüfung untergräbt.

# Was dies in der Praxis bedeutet

- **PCI-DSS:** Cyber Crucible verarbeitet, speichert oder überträgt keine Karteninhaberdaten und fällt daher als Verarbeiter von Kartendaten nicht in den Anwendungsbereich, während es dennoch die Kontrollziele der Endpunktsicherheit eines Kunden unterstützt.
- **HIPAA:** Da keine Kundeninhalte erfasst werden, vermeidet Cyber Crucible die Entstehung einer Verwahrungsbeziehung für geschützte Gesundheitsinformationen; eine Business Associate Agreement kann abgeschlossen werden, sofern ein Kunde dies benötigt.
- **ISO 27001 / CMMC / FedRAMP:** wird nicht gehalten und auch nicht als gehalten dargestellt.

# Was Cyber Crucible tatsächlich vorweisen kann

Eine unabhängige, objektive Validierung liegt dort vor, wo sie am wichtigsten ist – siehe *Welche unabhängige Sicherheitsvalidierung besitzt Cyber Crucible?* Framework-Verweise an anderer Stelle in dieser Wissensdatenbank sind selbst erstellte Zuordnungen, die einem Prüfer helfen, die Kontrollen von Cyber Crucible mit einem bereits genutzten Standard in Beziehung zu setzen; es handelt sich dabei nicht um Prüfurteile Dritter.

# Über welche unabhängige Sicherheitsvalidierung verfügt Cyber Crucible?

**Kurze Antwort:** Die Windows-Kernel-Treiber von Cyber Crucible werden im Rahmen von Microsofts Windows Hardware Compatibility Program (WHCP) objektiv geprüft und kryptografisch signiert. Dies ist eine externe, unabhängige Bestätigung der Qualität und Manipulationssicherheit der privilegiertesten Komponente des Produkts — dort, wo Korrektheit am wichtigsten ist.

## Warum WHCP von Bedeutung ist

Der Großteil des Endpoint-Marktes hat die Entwicklung auf Kernel-Ebene gemieden, weil sie tatsächlich schwierig und kostspielig ist. Cyber Crucible operiert bewusst auf Kernel-Ebene und reicht seine Treiber bei Microsofts Programm ein, damit eine externe Partei — nicht nur Cyber Crucible selbst — bestätigt, dass der sensibelste Code korrekt und manipulationssicher ist.

- Die Validierung ist **präzise auf den Treiber beschränkt** und wird nicht als Zertifizierung des Gesamtprodukts dargestellt.
- Es handelt sich um einen objektiven, wiederholbaren Test und nicht um ein subjektives Verwaltungsaudit.

## Wie es sich in das Gesamtbild einfügt

Für einen Prüfer, der üblicherweise nach einem SOC 2-Bericht sucht, stellt WHCP einen konkreten, unabhängigen Datenpunkt dar, den ein SOC 2-Bericht nicht liefert: die direkte Validierung der Kernel-Komponente. Es ergänzt die Nachweise zu den Kontrollen im vorbereiteten Anbieterpaket von Cyber Crucible, ersetzt sie jedoch nicht.

# Wie unterstützt Cyber Crucible GLBA- und Anbieteranforderungen für Finanzinstitute?

**Kurze Antwort:** Als Softwareanbieter für ein Finanzinstitut unterstützt Cyber Crucible die Verpflichtungen des Instituts im Rahmen der GLBA-Safeguards-Erwartungen und der interagency information-security guidelines – vor allem dadurch, dass es niemals die nicht-öffentlichen personenbezogenen Finanzinformationen (NPI) erfasst, zu deren Schutz diese Vorschriften verfasst wurden. Cyber Crucible ist ein Softwareanbieter und kein zugelassenes Finanzinstitut, wird daher selbst nicht geprüft; seine Kontrollen sind jedoch so ausgestaltet, dass sie im Rahmen des Drittanbieter-Risikoprogramms des Instituts überprüfbar sind.

## Wo die Architektur die Arbeit übernimmt

- **Keine NPI werden erfasst.** Das Produkt läuft auf Endpunkten, die NPI verarbeiten können, ohne diese zu extrahieren. Es gibt keine Verbraucher-Finanzinformationen, die Cyber Crucible nutzen, weitergeben oder erneut offenlegen könnte, was die Position zur GLBA Privacy Rule / Regulation P direkt unterstützt.
- **Dokumentiertes Sicherheitsprogramm.** Zugriffskontrolle, Verschlüsselung, Reaktion auf Sicherheitsverletzungen und Änderungskontrolle sind dokumentiert und nachweisbar – die Schutzmaßnahmen, die das Programm einer Bank von einem Dienstleister erwartet.
- **Sorgfaltspflicht-Nachweise vorhanden.** Ein vorbereitetes Anbieterpaket ist so strukturiert, dass es als Nachweis für die Due-Diligence- und laufende Überwachungspflichten dient, die eine Bank gemäß den aktuellen interagency third-party risk guidance benötigt.

## Die ehrliche Abgrenzung

Cyber Crucible unterstützt die Compliance-Verpflichtungen eines Kunden; es macht eine Organisation jedoch nicht allein compliant, und dies stellt keine Rechtsberatung dar. Spezifische, nachweistaugliche Details werden den Prüfern einer Bank unter einer Geheimhaltungsvereinbarung (NDA) zur Verfügung gestellt. Siehe auch *Erfüllt Cyber Crucible die Erwartungen von FFIEC und des Third-Party Risk Managements?*

# Erfüllt Cyber Crucible die Erwartungen von FFIEC und im Hinblick auf das Risikomanagement für Drittparteien?

**Kurze Antwort:** Cyber Crucible ist so konzipiert, dass es im Hinblick auf die Sicherheits-, Betriebs- und Geschäftskontinuitätserwartungen, die Prüfer an Banktechnologie stellen, überprüfbar ist, und das vorbereitete Anbieterpaket ist so aufgebaut, dass es als Sorgfaltspflicht-Nachweis dient, den ein Finanzinstitut gemäß der 2023 veröffentlichten interagency guidance zu Drittanbieterbeziehungen benötigt.

## Worauf sich das Programm einer Bank verlassen kann

- Kontrolldetails, die den in Standardfragebögen (SIG, CAIQ) enthaltenen Domänen sowie den SOC 2 Trust-Service Criteria und dem NIST CSF zugeordnet sind.
- Unabhängige Treibervalidierung (WHCP) als externe Qualitätsbestätigung.
- Eine dokumentierte, getestete Geschäftskontinuitätshaltung, mit der wichtigen Eigenschaft, dass der Endpunktschutz auch bei einem Ausfall des Management-Backends weiterhin aktiv bleibt.
- Versicherungsnachweise, Finanzinformationen und eine Liste der Unterauftragsverarbeiter, die Prüfern auf Anfrage zur Verfügung stehen.

## Warum die Architektur das Drittparteirisiko senkt

Die für den Vendor-Risk-Analysten einer Bank nützlichste Tatsache ist, dass Cyber Crucible niemals Kundendateien, Zugangsdaten oder Schlüssel erfasst. Die Daten, deren möglicher Missbrauch durch einen Anbieter einen Prüfer beunruhigt, befinden sich gar nicht erst im Besitz von Cyber

Crucible, sodass ein Missbrauch ausgeschlossen ist. Dies stellt eine strukturelle Risikominderung dar, kein bloßes Versprechen, das Risiko gut zu verwalten.

# Auf welche Sicherheits- und Compliance-Frameworks richtet sich Cyber Crucible aus?

**Kurze Antwort:** Cyber Crucible ordnet seine Kontrollen dem NIST Cybersecurity Framework, den relevanten NIST SP 800-53-Kontrollfamilien und den CIS Critical Security Controls zu und stellt zudem, zur Erleichterung für Prüfer, eine Zuordnung zu den SOC 2 Trust-Service Criteria bereit. Dabei handelt es sich um **selbst bewertete Zuordnungen**, die es einem Prüfer ermöglichen sollen, die Kontrollen von Cyber Crucible mit einem ihm bekannten Standard in Beziehung zu setzen – nicht um Zertifizierungen oder Prüfungsurteile Dritter.

## Zuordnung, ehrlich dargestellt

| Framework | Status |
|---|---|
| NIST Cybersecurity Framework (CSF) | Kontrollen selbst zugeordnet; keine Zertifizierung |
| NIST SP 800-53-Kontrollfamilien | Zuordnung, soweit anwendbar; keine Autorisierung |
| CIS Critical Security Controls | Zugeordnet; nicht zertifiziert |
| SOC 2 Trust-Service Criteria | Zur Erleichterung für Prüfer zugeordnet; kein Bericht vorhanden |
| Microsoft WHCP (Treiber) | Vorhanden – eine unabhängige, externe Validierung |

## Warum diese Darstellung gewählt wird

Ein Anbieter, der Frameworks auflistet, für die er nicht geprüft wurde, lädt den Prüfer dazu ein, jeder anderen Antwort zu misstrauen. Cyber Crucible gibt klar an, was eine Zertifizierung ist (WHCP) und was eine selbst bewertete Zuordnung ist (der Rest), damit ein Prüfer jedes Element entsprechend gewichten kann.

# Verwendet Cyber Crucible KI, und handelt es sich dabei um ein großes Sprachmodell?

**Kurze Antwort:** Cyber Crucible verwendet firmeneigene KI — jedoch ausschließlich während der Entwicklung, nicht auf Ihrem Endpunkt, und es handelt sich nicht um ein großes Sprachmodell. Ihre Genetic AI ist ein Discovery-Tool zur Entwurfszeit, das den deterministischen Satz an Verhaltensvariablen identifiziert, die auf einen Angriff hinweisen. Diese Erkenntnisse werden zu festen, deterministischen Heuristiken auf Kernel-Ebene. Zur Laufzeit läuft keine KI, kein LLM und kein adaptives Modell auf dem Gerät.

# Warum dies eine stärkere Position ist, nicht eine schwächere

- **Kein Laufzeitmodell bedeutet keine Drift.** Das Verhalten am Endpunkt ist deterministisch, wiederholbar und testbar — nicht probabilistisch.
- **Keine Live-Inferenzfläche.** Es gibt kein Modell auf dem Gerät, das ein Angreifer manipulieren oder vergiften könnte.
- **Keine Kundendaten in irgendeinem Modell.** Kundeninhalte, Anmeldedaten und Schlüssel werden niemals zum Trainieren, Speisen oder Anpassen eines Modells verwendet, und keine Kundendaten verlassen den Endpunkt zur KI-Verarbeitung.

Für einen Prüfer bei Finanzinstituten oder regulierten Unternehmen ist dies in der Regel die KI-Antwort, die er sich erhofft: Leistungsfähigkeit ohne ein live laufendes, undurchsichtiges Modell, das Entscheidungen am Endpunkt trifft.

# Verwandte Themen

Siehe *Wie wird KI im Entwicklungslebenszyklus von Cyber Crucible gesteuert?* für Informationen darüber, wie die Arbeit zur Entwurfszeit kontrolliert wird.

# Wie wird KI im Entwicklungslebenszyklus von Cyber Crucible gesteuert?

**Kurze Antwort:** Da die Genetic AI von Cyber Crucible ausschließlich zur Entwurfszeit eingesetzt wird, unterliegt sie der Governance des sicheren Entwicklungslebenszyklus (SDLC) und nicht der eines produktiv laufenden Systems. Die Discovery-Arbeit erfolgt in einer kontrollierten internen Umgebung, ihre Ergebnisse werden validiert und in deterministische Kernel-Heuristiken übersetzt, und die resultierenden Treiber werden vor der Veröffentlichung unabhängig unter Microsoft WHCP signiert.

## Der gesteuerte Lebenszyklus

| Phase | Governance |
|---|---|
| Design | Sicherheitsanforderungen werden festgelegt; die KI-Discovery ist Teil der Design-Phase, im Rahmen des SDLC |
| Discovery | Genetic AI identifiziert deterministische, angriffsanzeigende Variablen ausschließlich anhand interner Forschungsdatensätze |
| Ableitung | Erkenntnisse werden zu festen, deterministischen Kernel-Heuristiken — es wird kein live laufendes Modell bereitgestellt |
| Validierung | Deterministische Ergebnisse sind reproduzierbar und testbar; Modelle und Treiber werden durch QA validiert |
| Freigabe | Windows-Treiber werden WHCP-signiert; Änderungen folgen einem formalen Change-Management |

## Daten und Integrität

Es werden keine Kundeninhalte, Zugangsdaten oder Schlüssel verwendet, um ein Modell zu trainieren, zu speisen oder abzustimmen. Die Modelle sind proprietär und werden intern entwickelt, ohne Abhängigkeit von Drittanbieter-Modellen. Die Modellintegrität wird durch Versionskontrolle, SDLC-/QA-Validierung und WHCP-Signierung sichergestellt; die Vertraulichkeit durch eine kontrollierte Entwicklungsumgebung.

# Wo werden die Daten von Cyber Crucible verarbeitet — werden sie in der Cloud gespeichert?

**Kurze Antwort:** Bedrohungsanalyse und -reaktion erfolgen lokal auf dem Endpunkt, nicht in der Cloud. Cyber Crucible sammelt keine Kundendateien, Anmeldedaten oder Schlüssel und speichert keine Kundeninhalte bei einem Drittanbieter-Public-Cloud-Dienst. Das Management- und Reporting-Backend läuft auf von Cyber Crucible betriebener Infrastruktur in den Vereinigten Staaten, und für Organisationen, die keinerlei externen Datenfluss zulassen dürfen, steht eine vollständig On-Premises- oder air-gapped-Bereitstellung zur Verfügung.

## Warum lokale Verarbeitung wichtig ist

- **Die Schutzentscheidung verlässt niemals das Gerät.** Detect–Decide–Respond läuft im Kernel auf dem Endpunkt, typischerweise in unter 200 Millisekunden, ohne dass im kritischen Pfad ein Umweg über die Cloud erfolgt.
- **Vom Backend unabhängiger Schutz.** Ein Ausfall des Management-Backends verringert nicht den Schutz des Endpunkts.
- **Wahlfreiheit bei der Bereitstellung.** Organisationen mit strengen Vorgaben zur Datenresidenz oder Datenhoheit können Cyber Crucible vollständig innerhalb ihrer eigenen gesicherten Infrastruktur betreiben.

## Worauf sich ein Prüfer verlassen kann

Da Kundeninhalte niemals erfasst werden, hat die Frage „Wohin gehen unsere Daten?" für die Kategorien mit dem höchsten Risiko eine einfache Antwort: Sie gehen nirgendwohin. Detaillierte Informationen zur Infrastruktur und zu Unterauftragsverarbeitern werden Prüfern unter NDA zur Verfügung gestellt.

# Wie sieht die Serviceverfügbarkeit und das Support-SLA von Cyber Crucible aus?

**Kurzantwort:** Das veröffentlichte Service Level Agreement von Cyber Crucible garantiert eine **monatliche Serviceverfügbarkeit von 99,9 %** (ausgenommen geplante Wartungsarbeiten und Ursachen außerhalb der angemessenen Kontrolle), mit einem definierten Abhilfeverfahren in Form von Gutschriften für Ausfallzeiten. Die Support-Reaktionszeiten sind nach Schweregrad gestaffelt und werden ab Eingang des Tickets über das Support-Portal gemessen.

## Ziele für Support-Reaktionszeiten

| Schweregrad | Beschreibung | Reaktion |
|---|---|---|
| SEV1 — Kritisch | Dienst ausgefallen oder Produktionsbetrieb kritisch beeinträchtigt; noch keine Umgehungslösung vorhanden | ≤ 2 Stunden |
| SEV2 — Schwerwiegend | Dienst so beeinträchtigt, dass Schutz oder Reaktion eingeschränkt sind | ≤ 4 Stunden |
| SEV3 — Gering | Dienst beeinträchtigt, ohne Schutz oder Reaktion zu beeinflussen | ≤ 12 Stunden |
| SEV4 — Gering | Unkritisches Problem, Informationsanfrage oder Verbesserungsvorschlag | ≤ 48 Stunden |

## Wo Sie es finden

Das vollständige Service Level Agreement ist öffentlich zugänglich unter cybercrucible.com/service-level-agreement, und Support-Tickets werden unter support.cybercrucible.com eingereicht. Für regulierte Kunden kann vertraglich ein verbindlicher Zeitrahmen für die Benachrichtigung bei Sicherheitsverletzungen oder Vorfällen festgelegt werden.

# Ein Hinweis zur Verfügbarkeit

Da der Endpunktschutz lokal läuft, bezieht sich der Verfügbarkeitswert auf das Management- und Berichts-Backend. Der Schutz auf dem Gerät selbst bleibt auch dann bestehen, wenn das Backend vorübergehend nicht verfügbar ist.

# Wie geht Cyber Crucible mit Datenspeicherung und -löschung um?

**Kurze Antwort:** Cyber Crucible minimiert, was gespeichert wird, und bewahrt Daten nur so lange auf, wie es zur Erbringung des Dienstes erforderlich ist. Kundeninhalte, Anmeldedaten oder Schlüssel werden von vornherein nie erfasst, sodass für die risikoreichsten Kategorien nichts zum Aufbewahren vorhanden ist. Verhaltensbezogene Telemetriedaten und abgeleitete Sicherheitsmetadaten werden nach festgelegten Zeitplänen gelöscht, und am Ende eines Vertrags werden alle zugehörigen Daten zur Löschung bereitgestellt, mit entsprechender Bestätigung.

## Das Prinzip

- **Zuerst minimieren.** Die sensibelsten Daten werden nie erfasst, sodass in diesen Kategorien nichts aufzubewahren oder zu vernichten ist.
- **Zweckgebundene Aufbewahrung.** Verhaltensbezogene Telemetriedaten und Sicherheitsmetadaten werden nur so lange aufbewahrt, wie sie der Erkennung, Untersuchung und Berichterstattung dienen, und werden anschließend gelöscht.
- **Löschung bei Vertragsende.** Am Ende des Vertrags werden zugehörige Daten zur Löschung bereitgestellt, und Cyber Crucible stellt eine Bestätigung aus.

## Was dokumentiert ist

Ein dokumentierter Vernichtungsprozess umfasst sowohl gedruckte als auch elektronische Informationen. Die spezifischen Aufbewahrungsfristen nach Datentyp werden Prüfern unter NDA zur Verfügung gestellt und können vertraglich weiter eingeschränkt werden.

# Verfügt Cyber Crucible über einen Datenschutzbeauftragten?

**Kurze Antwort:** Ja. Cyber Crucible hat einen beauftragten Datenschutzbeauftragten (DPO) engagiert, der über länderübergreifende Expertise verfügt, die sich über die EU/UK-DSGVO, den kalifornischen CCPA/CPRA, HIPAA, PCI-DSS sowie globale Datenschutzregelungen einschließlich des saudi-arabischen PDPL erstreckt. Der DPO ist über den überwachten Posteingang **dpo@cybercrucible.com** erreichbar.

# Was der DPO abdeckt

- Das Datenschutzprogramm und Auftragsverarbeitungsverträge.
- Datenschutz-Folgenabschätzungen und Bewertungen von Transferrisiken, einschließlich Standardvertragsklauseln für grenzüberschreitende Übermittlungen.
- Entscheidungen zur Meldepflicht bei Datenschutzverletzungen sowie Unterstützung bei den eigenen Meldepflichten eines Kunden.
- Ein sachkundiger Ansprechpartner für Datenschutz- und Compliance-Fragen während des Beschaffungsprozesses.

# Warum ein beauftragter DPO mit globaler Expertise

Mehrere Regelwerke außerhalb der USA – darunter der saudi-arabische PDPL – können restriktiver sein als das derzeitige US-Recht. Durch die Beauftragung eines DPO, der mit der DSGVO, dem CCPA/CPRA, HIPAA und globalen PDPLs vertraut ist, kann Cyber Crucible Kunden nach dem strengeren Standard unterstützen, der die US-Mindestanforderungen in der Regel als Teilmenge erfüllt.

# Unterliegt Cyber Crucible den US-Exportkontrollen?

**Kurze Antwort:** Ja — die Software von Cyber Crucible unterliegt den Export Administration Regulations (EAR) des US-Handelsministeriums (Department of Commerce). Sie unterliegt **nicht** der ITAR-Kontrolle und wird nicht vom Außenministerium (Department of State) verwaltet. Für die Bereitstellung der Software an Kunden ist keine besondere Lizenz erforderlich, und die Exportklassifizierung sowie die Prüfung erfolgen im Rahmen des Compliance-Programms von Cyber Crucible.

# Was das für Käufer bedeutet

- **EAR, nicht ITAR.** Das Produkt unterliegt der Zuständigkeit des Handelsministeriums, dem Rahmenwerk, das für die meisten kommerziellen, verschlüsselungsfähigen Softwareprodukte gilt — nicht dem Regime für Verteidigungsgüter.
- **Patentiert und geprüft.** Die Technologie wurde nach einer Prüfung durch das US-Patent- und Markenamt (US Patent and Trademark Office), die auch eine Prüfung durch das Verteidigungsministerium (Department of Defense) umfasste, international patentiert.
- **Keine Lizenzierungshürde.** Die Bereitstellung der Software an einen Kunden erfordert keine besondere Exportlizenz.

Details zur Exportklassifizierung stehen Prüfern auf Anfrage zur Verfügung.

# Wie reduziert Cyber Crucible das Dritt- und Anbieterrisiko für regulierte Kunden?

**Kurze Antwort:** Indem das Risiko beseitigt und nicht nur verwaltet wird. Die drei Tatsachen, die die schwierigsten Fragen zum Anbieterrisiko beantworten, sind: Cyber Crucible erfasst keine Kundeninhalte, Zugangsdaten oder Schlüssel; der Schutz läuft lokal und übersteht jeden Backend-Ausfall; und die KI existiert ausschließlich in der Entwicklung, niemals auf Ihrem Endpunkt. Zusammen verkleinern diese Faktoren die Angriffsfläche, die eine Due-Diligence-Prüfung untersuchen soll.

## Die drei strukturellen Risikominderer

- **Keine Inhalte.** Es werden niemals Kundendateien, Zugangsdaten oder Schlüssel erfasst. Diese eine Tatsache beantwortet die Fragenkomplexe zu PCI, vertraulichen Daten und „was passiert, wenn Sie kompromittiert werden“ — die Daten sind schlicht nicht vorhanden, um verloren zu gehen.
- **Backend-unabhängiger Schutz.** Detect–Decide–Respond läuft lokal, mit einem effektiven Recovery-Time-Objective von null auf dem Endpunkt. Ein vollständiger Backend-Ausfall mindert den Schutz nicht.
- **Deterministische KI.** KI wird ausschließlich in der Entwicklung eingesetzt; zur Laufzeit laufen deterministische Heuristiken. Kein Live-Modell, kein Drift, testbare Ergebnisse.

## Unabhängige Bestätigung

Wo unabhängige Testate Gewicht haben, verweist Cyber Crucible auf das, was real ist: die Microsoft-WHCP-Treibersignierung sowie — für das verwaltete Backend — die Testate Dritter der Infrastrukturanbieter, auf die es sich stützt. Ohne eigenes SOC 2 tragen diese die Last ehrlich, statt überbewertet zu werden.

# Wie erhalte ich das Sicherheits-Due-Diligence-Paket von Cyber Crucible?

**Kurze Antwort:** Fordern Sie es bei **dpo@cybercrucible.com** an. Im Rahmen einer gegenseitigen Vertraulichkeitsvereinbarung (NDA) stellt Cyber Crucible ein vorbereitetes Sicherheitspaket für Anbieter zur Verfügung, das die Bereiche der Standardfragebögen (SIG, CAIQ) abdeckt und dort einspringt, wo ein Prüfer üblicherweise einen SOC-2-Bericht erwarten würde.

# Was das Paket und die dazugehörigen Unterlagen umfassen

- Ein vorbereitetes Sicherheits- und Vertrauenspaket für Anbieter: Architektur, Datenverarbeitung, Verschlüsselung, Zugriffsverwaltung, sichere Entwicklung, Vorfallreaktion, Geschäftskontinuität, regulatorische Ausrichtung sowie eine Zuordnung zu Kontroll-Frameworks.
- Einseitige Programmzusammenfassungen für Compliance, Audit sowie KI-/SDLC-Governance.
- Ein Versicherungsnachweis (Certificate of Insurance), ein W-9-Formular sowie Finanzinformationen, auf Anfrage erhältlich.
- Standardvertragsklauseln (Standard Contractual Clauses), eine Transfer Risk Assessment sowie eine Auftragsverarbeitungsvereinbarung (Data Processing Agreement), auf Anfrage erhältlich.

# Öffentliche Dokumente, die Sie jetzt einsehen können

| Dokument | Fundstelle |
|---|---|
| Service Level Agreement | cybercrucible.com/service-level-agreement |
| Gegenseitige NDA | cybercrucible.com/mutualNDA |
| MSA & EULA | cybercrucible.com/msa-and-eula |

| Dokument | Fundstelle |
| --- | --- |
| Datenschutzrichtlinie | cybercrucible.com/privacy-policy |

Alles über die öffentlichen Vereinbarungen hinaus wird Prüfern im Rahmen einer NDA und unter Einhaltung angemessener Vertraulichkeitsmaßnahmen zur Verfügung gestellt.