Branchenspezifische Leitfäden zum Anbieterrisiko

Antworten zur Sicherheits-Due-Diligence für spezifische regulierte Branchen — Gesundheitswesen, Bildung, Behörden, Verteidigung, Versorgungsunternehmen, Finanzdienstleistungen, Einzelhandel, Recht und Versicherungen — aufbereitet für den Prüfer von Anbieterrisiken. Legt klar dar, was Cyber Crucible besitzt und was nicht.

Wie unterstützt Cyber Crucible HIPAA, und wird eine Business Associate Agreement unterzeichnet?

Kurze Antwort: Cyber Crucible unterstützt die HIPAA-Verpflichtungen einer Covered Entity in erster Linie dadurch, dass niemals geschützte Gesundheitsinformationen (PHI) erfasst werden. Die Analyse erfolgt lokal auf dem Endpunkt, sodass PHI für die Sicherheitsverarbeitung nicht in eine Drittanbieter-Cloud hochgeladen werden. Da Cyber Crucible keine PHI im Auftrag einer Covered Entity erstellt, empfängt, verwaltet oder überträgt, erfüllt es in der Regel nicht die Definition eines Business Associate — sofern jedoch der Risikoprozess eines Kunden dies erfordert, kann eine Business Associate Agreement abgeschlossen werden.

Warum die Architektur für das Gesundheitswesen geeignet ist

- **PHI verlässt für die Sicherheitsanalyse niemals das Gerät.** Viele anbietergehostete SOC/MDR-Lösungen laden Dateien, Schlüssel oder Telemetriedaten in eine Drittanbieter-Cloud hoch; Cyber Crucible analysiert auf dem Endpunkt, sodass diese Gefährdung vermieden wird.
- **Klinische Kontinuität.** Nur der bösartige Prozess wird angehalten — keine vollständige Systemisolierung oder erzwungener Neustart — sodass angeschlossene Geräte und klinische Systeme weiterlaufen, während ein Angriff neutralisiert wird.
- **Ransomware-Schutz ohne 24/7-SOC.** Die autonome Prävention stoppt Angriffe bereits vor der Ausführung, ohne dass Analysten erforderlich sind, die ein Krankenhaus möglicherweise nicht bereitstellen kann.

Die ehrliche Grenze

Cyber Crucible ist nicht „HIPAA-zertifiziert" — eine solche Zertifizierung gibt es nicht. Es unterstützt Ihr Compliance-Programm; Ihre Datenschutz- und Sicherheitsbeauftragten treffen die Entscheidung für Ihre Umgebung. Eine BAA ist auf Anfrage über **dpo@cybercrucible.com** erhältlich.

Wie unterstützt Cyber Crucible FERPA und den Datenschutz für Schülerdaten an Schulen und Universitäten?

Kurzantwort: Cyber Crucible unterstützt Bildungseinrichtungen auf zwei Arten: Es stoppt Ransomware autonom, ohne ein rund um die Uhr besetztes Security Operations Center zu benötigen, und – über FortressAI – bewertet es den Datenzugriff von KI-Tools direkt auf dem Gerät, sodass Schülerdaten und Familiendaten nicht versehentlich an ein öffentliches KI-System gelangen. Da die Analyse lokal erfolgt und keine Schülerdaten gesammelt werden, verbleiben geschützte Bildungsunterlagen innerhalb der Grenzen der Einrichtung.

Die zwei Bildungsprobleme, die adressiert werden

- **Ransomware ohne SOC.** Die Prävention auf Kernel-Ebene stoppt Angriffe in unter 200 Millisekunden – ohne dass Analysten eingestellt oder ein Vertrag für die permanente Überwachung finanziert werden müssen.
- **KI-Governance für den Unterricht.** FortressAI prüft jede Eingabeaufforderung auf dem Gerät, sodass geschützte Bildungsunterlagen und persönliche Familiendaten nicht an ein öffentliches KI-System gesendet werden – auch nicht als Trainingsdaten.

Hinweise zur Anbieterauswahl

- Cyber Crucible fungiert als „school official“/Dienstleister unter der Weisung der Einrichtung und verwendet Schülerdaten für keinerlei sekundäre Zwecke.
- Bundesstaatliche Datenschutzgesetze für Schülerdaten (zum Beispiel in Kalifornien, New York und Colorado) sehen zusätzliche Anbieterpflichten vor; das Design mit lokaler Verarbeitung und ohne Datensammlung unterstützt deren Einhaltung. Dokumentation ist unter NDA verfügbar.

Ist Cyber Crucible FedRAMP-autorisiert, und wie dient es Regierungsbehörden?

Kurze Antwort: Nein — Cyber Crucible verfügt derzeit über keine FedRAMP-Autorisierung und suggeriert dies auch nicht anderweitig. FedRAMP autorisiert Cloud-Dienstangebote, die Behördendaten vorhalten; das Modell von Cyber Crucible ist anders. Es läuft lokal auf dem Endpunkt und kann vollständig On-Premises oder air-gapped innerhalb der eigenen Grenzen der Behörde bereitgestellt werden, sodass Behördendaten diese Grenze niemals in Richtung einer Drittanbieter-Cloud verlassen.

Wie die Architektur zu Regierungsanforderungen passt

- **On-Premises-/Air-Gapped-Bereitstellung.** Die Plattform kann vollständig innerhalb der gesicherten Infrastruktur einer Behörde laufen, ohne externen Datenfluss — geeignet für klassifizierte, getrennte und hochsichere Umgebungen.
- **Keine Erfassung von Behördendaten.** Kundendaten, Anmeldeinformationen und Schlüssel werden niemals erfasst, wodurch ein Großteil dessen entfällt, was eine Cloud-Autorisierung schützen soll.
- **In den USA hergestellt und exportkontrolliert.** Die Software unterliegt den EAR-Bestimmungen des US-Handelsministeriums (nicht ITAR) und ist international patentiert, nach einer USPTO-Prüfung, die eine Überprüfung durch das Verteidigungsministerium einschloss.

Die ehrliche Grenze

Sofern eine Behörde eine spezifische Autorisierung (FedRAMP, StateRAMP) benötigt, verfügt Cyber Crucible derzeit nicht darüber; das On-Premises-Bereitstellungsmodell ist der Weg, um Daten innerhalb der Behördengrenze zu halten. Details zu Bereitstellung und Kontrolle werden unter NDA bereitgestellt.

Erfüllt Cyber Crucible die CMMC- und DFARS-Anforderungen für die Defense Industrial Base?

Kurze Antwort: Cyber Crucible ist nicht CMMC-zertifiziert, und das wird auch klar so kommuniziert. Es unterstützt die Verpflichtungen eines Defense-Auftragnehmers gemäß DFARS 252.204-7012 und CMMC in erster Linie dadurch, dass keine Controlled Unclassified Information (CUI) erfasst werden und dass eine On-Premises- oder Air-Gapped-Bereitstellung innerhalb der eigenen Grenzen des Auftragnehmers unterstützt wird, wo CUI unter der Kontrolle des Auftragnehmers verbleibt.

Wie die Verpflichtungen des Auftragnehmers unterstützt werden

- **Keine Erfassung von CUI.** Der Endpoint-Agent analysiert Verhalten lokal, ohne die geschützten Dateien zu extrahieren, sodass CUI nicht an Cyber Crucible übertragen wird.
- **Grenzwahrende Bereitstellung.** On-Premises- und Air-Gapped-Modelle halten alle Daten innerhalb der geprüften Grenzen des Auftragnehmers.
- **Endpoint-Schutzkontrollen.** Malware-/Ransomware-Prävention und Überwachung entsprechen den relevanten CMMC-Praktiken und NIST-SP-800-171-Kontrollen, die der Auftragnehmer umsetzen muss.
- **US-Lieferkette.** US-Daten werden von in den USA ansässigen Ressourcen verarbeitet; Offshore-Auftragnehmer verarbeiten keine US-Daten und entwickeln auch nicht die Agenten. Die Software unterliegt der EAR-Kontrolle, nicht der ITAR.

Die ehrliche Grenze

Die CMMC-Zertifizierung wird von der Umgebung des Auftragnehmers gehalten, nicht von einem einzelnen Sicherheitstool; Cyber Crucible ist eine Kontrolle, die mehrere 800-171-Anforderungen unterstützt, kein Ersatz für die Bewertung des Auftragnehmers. Detaillierte Zuordnungen sind unter NDA verfügbar.

Wie passt Cyber Crucible zu NERC CIP und der Sicherheit kritischer Infrastrukturen?

Kurzantwort: Cyber Crucible eignet sich für Umgebungen kritischer Infrastrukturen und Versorgungsunternehmen, da es Endpunkte autonom schützt und offline oder air-gapped betrieben werden kann, ohne Cloud-Abhängigkeit im Schutzpfad. Das passt zu BES Cyber Systems und anderen Umgebungen, in denen die Konnektivität eingeschränkt ist und Verfügbarkeit oberste Priorität hat.

Warum es zu Versorgungsunternehmen und kritischen Infrastrukturen passt

- **Offline-/Air-Gap-fähig.** Vollständiger Schutz ohne Internetverbindung, geeignet für isolierte OT-Netzwerke und Umspannwerke.
- **Verfügbarkeitserhaltende Reaktion.** Nur der bösartige Prozess wird angehalten, sodass betriebliche Systeme weiterlaufen — keine vollständige Systemsperrung während eines Vorfalls.
- **Lokale, deterministische Entscheidungen.** Detect-Decide-Respond läuft auf dem Gerät, ohne Cloud-Umweg und ohne live agierendes KI-Modell.

Hinweise zur Anbieterauswahl

Die NERC-CIP-Verpflichtungen liegen bei der registrierten Einheit, nicht bei einem einzelnen Anbieter; Cyber Crucible ist eine Kontrolle, die mehrere CIP-Ziele unterstützt (Malware-Prävention, Überwachung, Vorfallbehandlung). Es handelt sich nicht um eine registrierte Einheit, und es wird auch nicht als CIP-zertifiziert dargestellt. Unterstützende Dokumentation ist unter NDA verfügbar.

Wie richtet sich Cyber Crucible an IEC 62443 für industrielle Steuerungssysteme aus?

Kurze Antwort: Cyber Crucible unterstützt das Defense-in-Depth-Modell von IEC 62443 für industrielle Automatisierungs- und Steuerungssysteme, indem es einen autonomen, kernelbasierten Endpunktschutz hinzufügt, der die Produktion nicht unterbricht. Er läuft lokal, toleriert den Betrieb ohne Verbindung und setzt ausschließlich bösartige Prozesse aus, was der Betonung des Standards auf sowohl Sicherheit als auch betriebliche Verfügbarkeit entspricht.

Wie es sich mit der Zielsetzung des Standards deckt

- **Zonen- und Verbindungsschutz.** Auf dem Endpunkt ansässige Prävention härtet die Geräte innerhalb einer Zone, ohne von einer Netzwerk-Rückmeldung abhängig zu sein.
- **Verfügbarkeit an erster Stelle.** Das selektive Aussetzen eines bösartigen Prozesses vermeidet die Anlagenausfallzeiten, die durch pauschale Eindämmung entstehen.
- **Funktioniert in Umgebungen mit geringer Konnektivität.** Geeignet für Produktionshallen, Logistikflotten und Edge-Standorte, an denen die Cloud-Konnektivität unzuverlässig oder bewusst nicht vorhanden ist.

Die ehrliche Grenze

Die IEC 62443-Zertifizierung gilt für Systeme und Prozesse, nicht für ein einzelnes Endpunkt-Tool; Cyber Crucible ist eine Komponente, die die Ziele des Standards unterstützt. Die Zuordnung der Kontrollen ist unter NDA verfügbar.

Wie unterstützt Cyber Crucible PCI-DSS für Einzelhandel und Gastgewerbe?

Kurzantwort: Cyber Crucible verarbeitet, speichert oder überträgt keine Karteninhaberdaten und fällt daher nicht in den Geltungsbereich als Verarbeiter von Kartendaten – unterstützt jedoch weiterhin die PCI-DSS-Kontrollziele des Händlers, insbesondere die Anforderung, Systeme vor Malware zu schützen. Es reduziert den PCI-Geltungsbereich, statt ihn zu erweitern.

Wie es die PCI-DSS-Ziele unterstützt

- **Malware-Schutz (Anforderung 5).** Autonome Prävention auf Kernel-Ebene stoppt Ransomware und speicherbasierte Angriffe auf Systeme innerhalb der Karteninhaberdaten-Umgebung.
- **Keine Erfassung von Karteninhaberdaten.** Der Agent beobachtet das Prozessverhalten und erfasst niemals Kartendaten, selbst auf Systemen, die Karten verarbeiten, wodurch der Prüfungsumfang nicht erweitert wird.
- **Kontinuität.** Es werden nur bösartige Prozesse angehalten, sodass Kassensysteme und Zahlungssysteme weiterhin funktionieren.

Hinweise zur Anbieterauswahl

Die PCI-DSS-Konformität liegt in der Verantwortung des Händlers und seines Prüfers; Cyber Crucible ist eine unterstützende Kontrolle, kein von einem QSA validierter Dienst. Es besitzt keine PCI-DSS-Zertifizierung und beansprucht auch keine solche.

Wie unterstützt Cyber Crucible Strafverfolgungsbehörden und CJIS-Umgebungen?

Kurzantwort: Cyber Crucible eignet sich für Criminal Justice Information Services (CJIS)-Umgebungen, da die Lösung Daten lokal verarbeitet, niemals kriminaltechnische Informationen (Criminal Justice Information, CJI) erfasst und sowohl vor Ort als auch air-gapped innerhalb der Behördengrenze betrieben werden kann. US-Daten werden von US-basiertem Personal verarbeitet, was die Anforderungen der CJIS Security Policy an Personal und Datenverarbeitung unterstützt.

Warum die Architektur passt

- **CJI bleibt innerhalb der Grenze.** Es werden keine Kundendaten erfasst; die Analyse erfolgt auf dem Endpunkt, sodass CJI nicht an eine Drittanbieter-Cloud übertragen wird.
- **US-Personal für US-Daten.** Offshore-Auftragnehmer verarbeiten keine US-Daten und entwickeln nicht die Agenten.
- **Verschlüsselung und Zugriffskontrolle.** Starke Authentifizierung, rollenbasierter Zugriff und Verschlüsselung unterstützen die technischen Kontrollen der Richtlinie.

Die ehrliche Abgrenzung

Die CJIS Security Policy wird von der jeweiligen Behörde und ihrer staatlichen CJIS Systems Agency durchgesetzt; Cyber Crucible unterstützt mehrere ihrer Kontrollbereiche, stellt selbst jedoch keine CJIS-„Zertifizierung“ dar. Details zur Personalüberprüfung und zu den Kontrollen sind unter NDA verfügbar.

Wie unterstützt Cyber Crucible Versicherer und Anforderungen an das Cyber-Underwriting?

Kurze Antwort: Cyber Crucible stärkt die Cyber-Versicherungsposition eines Unternehmens, da es die Kontrollen liefert, die Underwriter heute verlangen – autonome Ransomware-Prävention, Endpunktschutz und MFA-gestützten Zugriff – und gleichzeitig die Schadensoberfläche reduziert, indem es niemals Daten erfasst, die ein Angreifer monetarisieren könnte. Für Versicherer als Kunden schützt dasselbe Design mit lokaler Verarbeitung und ohne Datensammlung auch die Daten der Versicherungsnehmer.

Warum das beim Underwriting hilft

- **Ransomware-Prävention, nicht nur Erkennung.** Underwriter unterscheiden zunehmend zwischen Prävention und Erkennung; die Unterbindung vor der Ausführung ist die stärkere Kontrolle.
- **Reduzierte Breach-Exposition.** Da Kundendateien, Zugangsdaten und Schlüssel niemals erfasst werden, fällt die Antwort auf die Frage „Was, wenn Sie kompromittiert werden?" deutlich geringer aus.
- **Vorstandsreife Berichterstattung.** Prävention verringert die Offenlegungsexposition, was sowohl für Underwriter als auch für Vorstände relevant ist.

Hinweise zur Anbieterauswahl

Für einen Versicherer, der Cyber Crucible als eigenen Anbieter bewertet, unterstützen die Rolle als Auftragsverarbeiter, die Datenminimierung und die On-Premises-Option die Pflichten zum Schutz der Daten der Versicherungsnehmer. Die Dokumentation ist unter NDA verfügbar.

Wie schützt Cyber Crucible die Vertraulichkeit von Anwaltskanzleien und Unternehmen aus dem Bereich der professionellen Dienstleistungen?

Kurze Antwort: Cyber Crucible schützt privilegiertes und vertrauliches Mandantenmaterial, indem die Analyse auf dem Endgerät verbleibt und niemals Dateien, Anmeldeinformationen oder Schlüssel gesammelt werden – so werden Mandantengeheimnisse im Zuge des Schutzes nicht einer Drittanbieter-Cloud ausgesetzt. Es stoppt Ransomware und Infostealer autonom, was für Kanzleien ohne großes Sicherheitsteam von Bedeutung ist.

Warum es zu professionellen Dienstleistungen passt

- **Vertraulichkeit von Grund auf.** Keine Mandantendokumente verlassen das Gerät zur Sicherheitsverarbeitung; es gibt keine beim Anbieter gespeicherte Kopie, die vorgeladen oder kompromittiert werden könnte.
- **Schutz vor Identitäts- und Datendiebstahl.** Infostealer, die es auf Sitzungs-Token und Anmeldeinformationen abgesehen haben, werden abgefangen, bevor Daten das Gerät verlassen.
- **Geringer Betriebsaufwand.** Autonome Prävention funktioniert ohne einen rund um die Uhr besetzten SOC.

Hinweise zur Anbieterauswahl

Ethische Vertraulichkeitspflichten und, bei vielen Kanzleien, Zusatzvereinbarungen zur Mandantensicherheit führen zu einer genauen Prüfung der Anbieter; das Modell ohne Datensammlung und mit lokaler Verarbeitung unterstützt beides. Eine Auftragsverarbeitungsvereinbarung ist auf Anfrage erhältlich.