??????? ??????? ???????? ?????? ???????

كيف تجيب Cyber Crucible على اسئلة حول بيانات مخاطر الموردين الخاصة بالمؤسسات والمؤسسات المالية — ما تحتفظ به وما لا تحتفظ به، وكيف تدعم الالتزامات التنظيمية، وكيف يتم حوكمة الذكاء الاصطناعي، ومستويات الخدمة، وكيف تقلل بنيتها المعمارية من مخاطر الأطراف الثالثة. موضح بوضوح وأمانة.

- هل تمتلك Cyber Crucible تقرير SOC 2؟
- هل Cyber Crucible حاصلة على شهادة ISO 27001 أو PCI-DSS أو CMMC أو FedRAMP؟
- ما هو التحقق الأمني المستقل الذي تمتلكه Cyber Crucible؟
- كيف تدعم Cyber Crucible متطلبات GLBA ومتطلبات الموردين الخاصة بالمؤسسات المالية؟
- كيف تدعم Cyber Crucible متطلبات FFIEC وتوقعات إدارة مخاطر الأطراف الثالثة؟
- ما هي أطر الأمن والامتثال التي تتوافق معها Cyber Crucible؟
- هل تستخدم Cyber Crucible الذكاء الاصطناعي، وهل هو نموذج لغوي كبير؟
- كيف تُحكَم الذكاء الاصطناعي ضمن دورة حياة التطوير في Cyber Crucible؟
- أين تتم معالجة بيانات Cyber Crucible — وهل يتم تخزينها في السحابة؟
- ما هو مستوى توفر الخدمة واتفاقية مستوى دعم Cyber Crucible؟
- كيف تتعامل Cyber Crucible مع الاحتفاظ بالبيانات وحذفها؟
- هل تمتلك Cyber Crucible مسؤولاً عن خصوصية البيانات؟
- هل تخضع Cyber Crucible للوائح الرقابة على الصادرات الأمريكية؟
- كيف تقلل Cyber Crucible مخاطر الأطراف الثالثة والموردين لدى الجهات المنظّمة والخاضعة للرقابة؟
- كيف أحصل على حزمة العناية الواجبة الأمنية الخاصة بـ Cyber Crucible؟

?? ????? Cyber Crucible ????? SOC 2?

الإجابة المختصرة: لا. لا تمتلك Cyber Crucible حاليًا شهادة SOC 2، وهي تصرّح بذلك بوضوح بدلًا من الإيحاء بغير ذلك. والسبب معماري بطبيعته: فـ Cyber Crucible هي منتج برمجي يُنفَّذ محليًا، وليست جهة وصاية سحابية على بيانات العملاء، لذا فإن نموذج منظمة الخدمة الخاص بـ SOC 2 — الذي يشهد على كيفية تخزين مزوّد الخدمة ومعالجته ونقله لبيانات □□□□□□ على أنظمته الخاصة — لا ينطبق عليها بشكل مباشر.

????? ?? ???? ???? ??????? ??? ???

يشهد SOC 2 على ضوابط منظمة الخدمة التي تحتفظ ببيانات العملاء. ويزيل تصميم Cyber Crucible هذا الافتراض الأساسي:

- يعمل الكشف عن التهديدات والاستجابة لها على مستوى نقطة النهاية، وعلى مستوى النواة (kernel)، على جهاز العميل نفسه.
- لا تُجمَّع ملفات العميل ولا بيانات اعتماده ولا مفاتيح التشفير ولا رموز الجلسة (session tokens) أبدًا، ولا تُنقل أو تُخزَّن من قِبل Cyber Crucible.
- يمكن نشر المنصة بالكامل داخل مقر العميل أو في بيئة معزولة تمامًا (air-gapped)، ضمن البنية التحتية الخاصة بالعميل.

ولأن أعلى فئات البيانات خطورةً لا تكون أبدًا في عهدة Cyber Crucible، فإن جزءًا كبيرًا من مساحة مخاطر المورّد التي يهدف SOC 2 إلى معالجتها تُزال بحكم التصميم بدلًا من مجرد ضبطها.

?? ???? ??? ????

بالنسبة للمراجعين الذين يعملون وفق استباين، توفّر Cyber Crucible حزمة أمان معدّة مسبقًا للمورّدين تقدّم أدلة الضوابط الأساسية مباشرةً، وتُطابق ضوابطها مع معايير خدمة الثقة الخاصة بـ SOC 2 (Trust-Service Criteria) وإطار عمل الأمن السيبراني الخاص بـ NIST، بحيث يمكن للمراجع إكمال استباين قياسي استنادًا إليها. وتتوفر هذه الحزمة بموجب اتفاقية عدم إفصاح متبادلة (NDA) من خلال **dpo@cybercrucible.com**.

وتبقى خارطة طريق الضمان قيد التقييم المستمر بما يتماشى مع احتياجات العملاء؛ وسيتم تحديث هذه الصفحة في حال تغيّر هذا الموقف.

?? Cyber Crucible ????? ??? ????? ISO 27001 ?? PCI-DSS ?? CMC ?? FedRAMP?

الإجابة المختصرة: لا. لم تحصل Cyber Crucible على شهادة أو تفويض ISO/IEC 27001 أو PCI-DSS أو HIPAA أو CMC أو FedRAMP، ولا تدّعي حيازتها. وتذكر ذلك صراحةً، لأن ادّعاء بائع الحوصل على شهادة لا يملكها هو بالضبط نوع التناقض الذي يقوّض الثقة في مراجعة العناية الواجبة.

لمعرفة المزيد: [منع برامج الفدية وسرقة بيانات الاعتماد على مستوى نواة نظام التشغيل (Cyber Crucible Core)]

???? ???? ??? ??????

- **PCI-DSS:** لا تقوم Cyber Crucible بمعالجة أو تخزين أو نقل بيانات حاملي البطاقات، لذا فهي خارج نطاق كونها معالجًا لبيانات البطاقات، مع استمرارها في دعم أهداف الرقابة الأمنية لنقاط النهاية لدى العميل.
- **HIPAA:** نظرًا لعدم جمع أي محتوى خاص بالعميل، تتجنب Cyber Crucible إنشاء علاقة حيازة لمعلومات صحية محمية؛ ويمكن توقيع اتفاقية شريك أعمال (Business Associate Agreement) في حال احتاج العميل إلى ذلك.
- **ISO 27001 / CMMC / FedRAMP:** غير حاصلة عليها، ولا يُدّعى امتلاكها.

?? ????? Cyber Crucible ?????

يوجد تحقق مستقل وموضوعي حيثما كان ذلك أكثر أهمية — راجع □□ □□ □□□□□□ □□□□□□ □□□□□□□ □□□□ □□□□□□ *Cyber Crucible*□ أما الإشارات إلى الأطر المرجعية الواردة في مواضع أخرى من قاعدة المعرفة هذه فهي تعيينات ذاتية التقييم تساعد المراجع على ربط ضوابط Cyber Crucible بمعيار يستخدمه بالفعل؛ وهي ليست آراء تدقيق من طرف ثالث.

?? ?? ?????? ?????? ??????? ???? ?????? Cyber Crucible?

الإجابة المختصرة: يتم اختبار برامج تشغيل نواة نظام Windows الخاصة بـ Cyber Crucible بشكل موضوعي وتوقيعها تشفيريًا بموجب برنامج Microsoft لتوافق أجهزة Windows (WHCP). وهذا يمثل تصديقًا خارجيًا ومستقلًا على جودة أهم مكون في المنتج ومقاومته للعبث — وهو الكود الذي تُعد فيه الدقة أكثر أهمية من أي مكان آخر.

????? ???? WHCP ?? ?????

تجنّب معظم سوق حماية نقاط النهاية (endpoint) تطوير الحلول على مستوى النواة لأن ذلك يتطلب جهدًا وتكلفة كبيرين بالفعل. تعمل Cyber Crucible عمدًا على مستوى النواة، وتُخضع برامج التشغيل الخاصة بها لبرنامج Microsoft بحيث تقوم جهة خارجية — وليس Cyber Crucible وحدها — بالتحقق من أن الكود الأكثر حساسية صحيح ومقاوم للعبث.

- عملية التحقق **محددة النطاق بدقة على برنامج التشغيل**، والا تُقدّم على أنها شهادة تشمل المنتج بأكمله.
- إنها اختبار موضوعي وقابل للتكرار، وليست تدقيقًا إداريًا ذاتيًا.

??? ????? ??? ??? ?????? ??????

بالنسبة للمراجع المعتاد على البحث عن تقرير SOC 2، يمثل WHCP نقطة بيانات مستقلة ومألوفة لا يوفره تقرير SOC 2: وهي التحقق المباشر من مكوّن النواة. وهو يكمّل — ولا يحل محل — أدلة الضوابط الواردة في حزمة الموردين المُعدة من قبل Cyber Crucible.

??? ???? Cyber Crucible ??????? GLBA ???????? ???????? ?????? ????????? ????????

إجابة موجزة: بصفتها مزودة لخدمة برمجية لمؤسسة مالية، تدعم Cyber Crucible التزامات المؤسسة بموجب توقعات ضمانات GLBA (GLBA Safeguards) والإرشادات المشتركة بين الوكالات الخاصة بأمن المعلومات — وذلك بشكل أساسي من خلال عدم جمع معلومات المعلومات الشخصية غير العامة (NPI) التي وُضعت هذه القواعد لحمايتها. Cyber Crucible مزود برمجيات، وليست مؤسسة مالية مرخصة، لذا فهي ليست خاضعة للفحص بحد ذاتها؛ بل صُممت ضوابطها لتكون قابلة للفحص كجزء من برنامج إدارة مخاطر الأطراف الثالثة الخاص بالمؤسسة.

لمعرفة المزيد: حماية المصارف والمؤسسات المالية من برامج الفدية وبرامج سرقة المعلومات

??? ???? ?????? ????????? ??????

- **عدم جمع معلومات NPI.** يعمل المنتج على نقاط النهاية التي قد تتعامل مع معلومات NPI دون استخراجها. لا توجد معلومات مالية استهلاكية لتستخدمها Cyber Crucible أو تشاركها أو تعيد الإفصاح عنها، وهو ما يدعم بشكل مباشر موقف قاعدة الخصوصية الخاصة بـ GLBA / اللائحة P (Regulation P).
- **برنامج أمني موثّق.** التحكم في الوصول، والتشفير، والاستجابة للاختراقات، والتحكم في التغييرات، جميعها موثّقة وقابلة للإثبات — وهي الضمانات التي يبحث عنها برنامج البنك لدى مزود الخدمة.
- **أدلة العناية الواجبة جاهزة.** تم تصميم حزمة الموردين المُعدّة لتكون بمثابة أدلة العناية الواجبة والمراقبة المستمرة التي يحتاجها البنك بموجب الإرشادات الحالية المشتركة بين الوكالات بشأن مخاطر الأطراف الثالثة.

?????? ???????

تدعم Cyber Crucible التزامات الامتثال الخاصة بالعميل؛ لكنها لا تجعل، بحد ذاتها، المؤسسة ممتثلة، وهذا ليس استشارة قانونية. تُقدّم التفاصيل المحددة والقابلة للإثبات إلى مراجعي البنك بموجب اتفاقية عدم إفصاح (NDA). راجع أيضاً □□ □□□□ *Cyber Crucible* □□□□□□ *FFIEC* □□□□□□ □□□□□ □□□□□□□ □□□□□□□□

??? ???? Cyber Crucible ??????? FFIEC ??????? ????? ????? ??????? ????????

إجابة موجزة: صُممت Cyber Crucible لتكون قابلة للفحص وفق توقعات الأمن والعمليات واستمرارية الأعمال التي يطبقها المدققون على تقنية البنوك، كما أن حزمة الموردين المُعدة مسبقاً منظمة لتكون بمثابة أدلة العناية الواجبة التي تحتاجها المؤسسة المالية بموجب التوجيهات المشتركة بين الوكالات لعام 2023 بشأن علاقات الأطراف الثالثة.

لمعرفة المزيد: حماية المصارف والمؤسسات المالية من برامج الفدية وبرامج سرقة المعلومات

?? ???? ??????? ????? ???????? ????

- تفاصيل الضوابط مُرتبطة بالمجالات الموجودة في الاستبيانات القياسية (SIG وCAIQ) وبمعايير خدمات الثقة الخاصة بـ SOC 2 وإطار عمل NIST CSF.
- التحقق المستقل من برامج التشغيل (WHCP) كشهادة جودة خارجية.
- وضعية موثقة ومُختبرة لاستمرارية الأعمال، مع خاصية مهمة وهي استمرار حماية نقاط النهاية حتى أثناء انقطاع الواجهة الخلفية للإدارة.
- أدلة التأمين، والمعلومات المالية، وقائمة معالجي الفرعيين المتاحة للمراجعين عند الطلب.

????? ????? ?????? ????????? ?? ????? ??????? ???????

الحقيقة الأكثر فائدة بالنسبة لمحلل مخاطر الموردين في البنك هي أن Cyber Crucible ال تجمع أبداً ملفات العملاء أو بيانات الاعتماد أو المفاتيح. فالبيانات التي يقلق المراجع من سوء تعامل المورد معها ليست في عهدة Cyber Crucible أصلاً حتى يُساء التعامل معها. وهذا يُمثل تخفيضاً بنيوياً للمخاطر، وليس مجرد وعد بإدارتها بشكل جيد.

?? ?? ??? ????? ????????? ???? ?????? ???? Cyber Crucible?

إجابة موجزة: تقوم Cyber Crucible بربط ضوابطها مع إطار عمل الأمن السيبراني الصادر عن NIST (NIST Cybersecurity Framework)، وعائلات الضوابط ذات الصلة ضمن NIST SP 800-53، وضوابط الأمان الحرجة الصادرة عن CIS (CIS Critical Security Controls)، كما تربطها بمعايير خدمات الثقة الخاصة بـ SOC 2 تسهيلاً على المراجع. هذه **محاذاة قائمة على التقييم الذاتي**، تُقدّم لتمكين المراجع من ربط ضوابط Cyber Crucible بمعيار يعرفه — وليست شهادات اعتماد أو آراء تدقيق صادرة عن جهة خارجية.

????????? ?????? ????

الإطار	الحالة
إطار عمل الأمن السيبراني الصادر عن NIST (CSF)	ضوابط مربوطة ذاتياً؛ ليست شهادة اعتماد
عائلات الضوابط ضمن NIST SP 800-53	متوافقة حيثما ينطبق ذلك؛ ليست تصريحاً رسمياً
ضوابط الأمان الحرجة الصادرة عن CIS	متوافقة؛ غير معتمدة
معايير خدمات الثقة الخاصة بـ SOC 2	مربوطة تسهيلاً على المراجع؛ لا يوجد تقرير محتفظ به
برنامج WHCP من Microsoft (لتعريف التشغيل)	معتمَد — تحقق مستقل وخارجي

??? ??? ??????? ?? ?????

إن أي مورّد يُدرج أطراً لم يخضع لتدقيق بشأنها يدفع المراجع إلى الشك في كل إجابة أخرى يقدمها. توضح Cyber Crucible بدقة ما يمثل شهادة اعتماد فعلية (WHCP) وما يمثل محاذاة قائمة على التقييم الذاتي (البقية)، بحيث يتمكن المراجع من تقييم كل منها بالشكل المناسب.

?? ?????? Cyber Crucible ?????? ??????????? ??? ?? ????? ???? ?????

الإجابة المختصرة: تستخدم Cyber Crucible ذكاءً اصطناعيًا مملوكًا لها — ولكن فقط أثناء مرحلة التطوير، وليس على نقطة النهاية الخاصة بك، وهو ليس نموذجًا لغويًا كبيرًا. يُعدّ Genetic AI الخاص بها أداة اكتشاف تُستخدم وقت التصميم لتحديد المجموعة الحتمية من المتغيرات السلوكية التي تشير إلى وجود هجوم. تتحول هذه النتائج إلى قواعد استدلال (heuristics) ثابتة وحتمية على مستوى النواة (kernel). وفي وقت التشغيل، لا يعمل أي ذكاء اصطناعي، ولا أي نموذج لغوي كبير، ولا أي نموذج تكيّفي على الجهاز.

????? ???? ??? ?????? ????? ?? ????

- **عدم وجود نموذج وقت التشغيل يعني عدم وجود انحراف (drift).** سلوك نقطة النهاية حتمي، وقابل للتكرار، وقابل للاختبار — وليس احتماليًا.
- **لا توجد واجهة استدلال حية.** لا يوجد نموذج على الجهاز يمكن للمهاجم التلاعب به أو تسميمه.
- **لا توجد بيانات عملاء في أي نموذج.** لا يُستخدم محتوى العملاء أو بيانات الاعتماد أو المفاتيح مطلقًا لتدريب أو تغذية أو ضبط أي نموذج، ولا تغادر أي بيانات عملاء نقطة النهاية لأغراض معالجة الذكاء الاصطناعي.

بالنسبة للمراجع في مؤسسة مالية أو جهة خاضعة للتنظيم، عادةً ما تكون هذه هي الإجابة التي يأملون سماعها بشأن الذكاء الاصطناعي: قدرة فعلية دون وجود نموذج حي وغير شفاف يتخذ القرارات على نقطة النهاية.

?? ???

راجع [illegible] *Cyber Crucible* لمعرفة كيفية ضبط العمل في مرحلة التصميم.

??? ?????? ?????? ????????? ??? ???? ???? ??????? ?? Cyber Crucible?

إجابة موجزة: نظرًا لأن Genetic AI الخاص بـ Cyber Crucible يُستخدم فقط في وقت التصميم، فإنه يُحكَم ضمن دورة حياة التطوير الآمن (SDLC) بدلًا من كونه نظامًا حيًا قيد التشغيل الفعلي. تجري أعمال الاكتشاف في بيئة داخلية خاضعة للتحكم، ويتم التحقق من صحة مخرجاتها وترجمتها إلى استدلالات حتمية (deterministic) على مستوى النواة (kernel heuristics)، ويتم توقيع برامج التشغيل الناتجة بشكل مستقل بموجب Microsoft WHCP قبل إصدارها.

???? ?????? ??????? ???????

المرحلة	الحوكمة
التصميم	تُحدّد متطلبات الأمان؛ ويُعدّ اكتشاف الذكاء الاصطناعي جزءًا من مرحلة التصميم، ضمن دورة حياة التطوير الآمن (SDLC)
الاكتشاف	يحدد Genetic AI المتغيرات الحتمية الدالة على الهجمات باستخدام مجموعات بيانات بحثية داخلية فقط
الاشتقاق	تتحول النتائج إلى استدلالات ثابتة وحتمية على مستوى النواة (kernel heuristics) — ولا يتم نشر أي نموذج حي
التحقق	النتائج الحتمية قابلة للتكرار والاختبار؛ ويتم التحقق من صحة النماذج وبرامج التشغيل من خلال ضمان الجودة (QA)
الإصدار	يتم توقيع برامج تشغيل Windows بموجب WHCP؛ وتخضع التغييرات لإدارة تغيير رسمية

???????? ????????

لا تُستخدم أي محتويات أو بيانات اعتماد أو مفاتيح خاصة بالعملاء لتدريب أو تغذية أو ضبط أي نموذج. النماذج مملوكة حصريًا ومبنية داخليًا، دون أي اعتماد على نماذج من جهات خارجية. يتم الحفاظ على سلامة النموذج من خلال التحكم في الإصدارات، والتحقق عبر دورة حياة التطوير الآمن/ضمان الجودة (SDLC/QA)، والتوقيع عبر WHCP؛ وتُحفظ السرية من خلال بيئة تطوير خاضعة للتحكم.

??? ??? ?????? ?????? Cyber Crucible — ??? ??? ??????? ?? ????????

إجابة موجزة: يتم تحليل التهديدات والاستجابة لها محليًا على نقطة النهاية (Endpoint)، وليس في السحابة. لا تقوم Cyber Crucible بجمع ملفات العملاء أو بيانات الاعتماد أو المفاتيح، ولا تقوم بتخزين محتوى العملاء لدى مزود سحابة عام تابع لجهة خارجية. تعمل البنية الخلفية للإدارة وإعداد التقارير على بنية تحتية تديرها Cyber Crucible داخل الولايات المتحدة، ويتوفر نشر محلي بالكامل (on-premises) أو معزول عن الشبكة (air-gapped) للمؤسسات التي تتطلب انعدام أي تدفق بيانات خارجي.

????? ???? ???????? ??????? ????

- **القرار الوقائي لا يغادر الجهاز أبدًا.** يعمل Detect-Decide-Respond داخل النواة (kernel) على نقطة النهاية، عادةً في أقل من 200 ميلي ثانية، دون أي اتصال بالسحابة ضمن المسار الحرج.
- **حماية مستقلة عن البنية الخلفية.** لا يؤدي انقطاع البنية الخلفية للإدارة إلى تقليل مستوى الحماية على نقطة النهاية.
- **حرية اختيار طريقة النشر.** يمكن للمؤسسات ذات المتطلبات الصارمة بشأن إقامة البيانات أو السيادة عليها تشغيل Cyber Crucible بالكامل داخل بنيتها التحتية المؤمّنة الخاصة.

?? ???? ????????? ???????? ????

نظرًا لأن محتوى العملاء لا يُجمع أبدًا، فإن الإجابة عن سؤال "إلى أين تذهب بياناتنا؟" بسيطة بالنسبة لأكثر الفئات حساسية: إنها لا تذهب إلى أي مكان. تُقدّم المعلومات التفصيلية المتعلقة بالبنية التحتية والجهات الفرعية المعالِجة للمُراجعين بموجب اتفاقية عدم إفصاح (NDA).

?? ?? ????? ???? ?????? ???????? ????? ??? Cyber Crucible?

الإجابة المختصرة: تلتزم اتفاقية مستوى الخدمة المنشورة لدى Cyber Crucible بـ **توفر خدمة شهري بنسبة 99.9%** (باستثناء أعمال الصيانة المجدولة والأسباب الخارجة عن سيطرتها المعقولة)، مع آلية تعويض محددة عن فترات التوقف. أوقات استجابة الدعم مصنفة حسب مستوى الخطورة، وتُقاس من لحظة إدخال التذكرة عبر بوابة الدعم.

????? ??? ??????? ?????

مستوى الخطورة	الوصف	زمن الاستجابة
SEV1 — حرج	توقف الخدمة أو تأثر الإنتاج بشكل حرج؛ لا يوجد حل بديل بعد	≤ ساعتان
SEV2 — كبير	تدهور الخدمة بطريقة تحد من الحماية أو الاستجابة	≤ 4 ساعات
SEV3 — بسيط	تدهور الخدمة دون التأثير على الحماية أو الاستجابة	≤ 12 ساعة
SEV4 — بسيط	مشكلة غير حرجة، أو طلب معلومات، أو تحسين مقترح	≤ 48 ساعة

??? ???? ?????? ?????

اتفاقية مستوى الخدمة الكاملة متاحة للعموم على cybercrucible.com/service-level-agreement، ويتم إدخال تذاكر الدعم عبر support.cybercrucible.com. يمكن تحديد إطار زمني ملزم تعاقديًا للإبلاغ عن الاختراقات أو الحوادث للعملاء الخاضعين للتنظيم.

?????? ??? ??????

نظرًا لأن حماية نقطة النهاية تعمل محليًا، فإن رقم التوفر ينطبق على الواجهة الخلفية للإدارة وإعداد التقارير. وتستمر الحماية على الجهاز نفسه حتى في حال عدم توفر الواجهة الخلفية مؤقتًا.

??? ?????? Cyber Crucible ?? ???????? ????????? ???????

إجابة موجزة: تعمل Cyber Crucible على تقليل ما تحتفظ به من بيانات إلى الحد الأدنى، والا تحتفظ بالبيانات إلا للمدة اللازمة لتقديم الخدمة. فهي لا تجمع أبدًا محتوى العميل أو بيانات الاعتماد أو المفاتيح في المقام الأول، وبالتالي لا يوجد شيء يجب الاحتفاظ به في هذه الفئات الأعلى خطورة. أما البيانات السلوكية والبيانات الوصفية الأمنية المشتقة، فيتم التخلص منها وفق جداول زمنية محددة، وعند انتهاء العقد تُتاح جميع البيانات المرتبطة به للحذف مع تقديم تأكيد بذلك.

??????

- **التقليل أولًا.** لا يتم جمع البيانات الأكثر حساسية على الإطلاق، وبالتالي لا يوجد شيء في تلك الفئات يجب الاحتفاظ به أو إتلافه.
- **الاحتفاظ بحسب الغرض.** يتم الاحتفاظ بالبيانات السلوكية والبيانات الوصفية الأمنية فقط طالما أنها تخدم أغراض الكشف والتحقيق وإعداد التقارير، ثم يتم التخلص منها تدريجيًا.
- **الحذف عند الخروج.** عند انتهاء العقد، تُتاح البيانات المرتبطة للحذف، وتقدم Cyber Crucible تأكيدًا بذلك.

?? ??? ??????

تغطي عملية إتلاف موثقة كلًا من المعلومات المطبوعة والإلكترونية. تُقدَّم فترات الاحتفاظ المحددة بحسب نوع البيانات إلى الجهات المرجعية بموجب اتفاقية عدم إفصاح (NDA)، ويمكن تشديدها بموجب العقد.

?? ????? Cyber Crucible ??????? ?? ?????? ?????????

الإجابة المختصرة: نعم. تعاقدت Cyber Crucible مع مسؤول خصوصية بيانات (DPO) يتمتع بخبرة تشمل عدة ولايات قضائية، بما في ذلك GDPR الأوروبي/البريطاني، وقانونَي CCPA/CPRA في كاليفورنيا، وHIPAA، وPCI-DSS، بالإضافة إلى أنظمة حماية البيانات العالمية بما فيها نظام حماية البيانات الشخصية السعودي (PDPL). يمكن التواصل مع مسؤول خصوصية البيانات عبر صندوق البريد الإلكتروني الخاضع للمراقبة **dpo@cybercrucible.com**.

?? ???? ????? ??? ????? ?????? ????????

- برنامج الخصوصية واتفاقيات معالجة البيانات.
- تقييمات تأثير حماية البيانات ومخاطر النقل، بما في ذلك البنود التعاقدية القياسية (Standard Contractual Clauses) الخاصة بعمليات النقل عبر الحدود.
- تحديد ما إذا كان يلزم الإخطار بالاختراقات، وتقديم الدعم للعملاء فيما يخص التزاماتهم الخاصة بالإخطار.
- نقطة اتصال ذات خبرة للإجابة على الأسئلة المتعلقة بالخصوصية والامتثال أثناء عمليات الشراء.

????? ??????? ?? ????? ?????? ?????? ?? ???? ??????

توجد عدة أنظمة خارج الولايات المتحدة — ومن بينها نظام PDPL السعودي — قد تكون أكثر تقييداً من القانون الأمريكي الحالي. فالتعاقد مع مسؤول خصوصية بيانات ملم بـ GDPR وCCPA/CPRA وHIPAA أو أنظمة PDPL العالمية يتيح لشركة Cyber Crucible دعم العملاء وفقاً للمعايير الأكثر صرامة، وهو ما يستوفي عادةً الحد الأدنى الأمريكي باعتباره جزءاً منه.

?? ???? Cyber Crucible ?????? ??????? ??? ???????? ??????????

الإجابة المختصرة: نعم — يخضع برنامج Cyber Crucible للوائح إدارة الصادرات (EAR) الصادرة عن وزارة التجارة الأمريكية. وهو **غير** خاضع لنظام ITAR والا تديره وزارة الخارجية الأمريكية. ال يلزم الحصول على ترخيص خاص لتوفير البرنامج للعملاء، ويتم التعامل مع تصنيف الصادرات والفحص كجزء من برنامج الامتثال الخاص بـ Cyber Crucible.

???? ???? ??? ??????? ???????

- **EAR وليس ITAR.** يخضع المنتج لولاية وزارة التجارة، وهو الإطار الذي ينطبق على معظم البرمجيات التجارية التي تحتوي على تشفير — وليس نظام المواد الدفاعية.
- **مسجّل ببراءة اختراع، وتمت مراجعته.** تم تسجيل براءة اختراع دولية للتقنية بعد مراجعة أجرتها مكتب براءات الاختراع والعلامات التجارية الأمريكي، شملت مراجعة من وزارة الدفاع.
- **لا يوجد عائق ترخيصي.** توفير البرنامج للعميل لا يتطلب الحصول على ترخيص تصدير خاص.

تفاصيل تصنيف الصادرات متاحة للمراجعين عند الطلب.

??? ???? Cyber Crucible ????? ??????? ??????? ????????? ??? ?????? ????????? ???????? ????????

إجابة موجزة: عبر إزالة المخاطرة بدلاً من مجرد إدارتها. الحقائق الثلاث التي تجيب عن أصعب أسئلة مخاطر الموردين هي: أن Cyber Crucible لا تجمع أي محتوى للعملاء أو بيانات اعتماد أو مفاتيح؛ وأن الحماية تعمل محلياً وتستمر حتى في حال انقطاع أي خدمة خلفية؛ وأن الذكاء الاصطناعي الخاص بها موجود فقط في مرحلة التطوير، ولا يُستخدم أبداً على جهاز الطرفي. تجتمع هذه العوامل لتقليص النطاق الذي تسعى مراجعة العناية الواجبة لفحصه.

????? ????? ??????? ???????? ???????

- **صفر محتوى.** لا يتم جمع أي ملفات للعملاء أو بيانات اعتماد أو مفاتيح إطلاقاً. هذه الحقيقة الواحدة تجيب عن أسئلة PCI، وأسئلة البيانات السرية، وأسئلة "ماذا لو تعرضتم للاختراق" — فالبيانات غير الموجودة أصلاً لا تُفقد.
- **حماية مستقلة عن البنية الخلفية.** يعمل Detect–Decide–Respond محلياً، بهدف زمن تعافٍ يساوي صفراً على الجهاز الطرفي. انقطاع كامل للبنية الخلفية لا يقلل من مستوى الحماية.
- **ذكاء اصطناعي حتمي.** يُستخدم الذكاء الاصطناعي في مرحلة التطوير فقط؛ بينما تعمل الخوارزميات الاستدلالية الحتمية أثناء التشغيل الفعلي. لا يوجد نموذج حي، ولا انحراف، والنتائج قابلة للاختبار.

??????? ???????

حيثما تحمل الشهادات المستقلة وزناً معتبراً، تشير Cyber Crucible إلى ما هو حقيقي وقائم: توقيع برامج التشغيل عبر Microsoft WHCP، وبالنسبة للبنية الخلفية المُدارة — الشهادات المستقلة الصادرة عن مزودي البنية التحتية الذين تعتمد عليهم. ومع عدم امتلاكها شهادة SOC 2 خاصة بها، فإن هذه العناصر تتحمل العبء بصدق دون مبالغة في عرضها.

??? ???? ??? ???? ??????? ??????? ??????? ?????? ?? Cyber Crucible?

الإجابة المختصرة: اطلبها من **dpo@cybercrucible.com**. بموجب اتفاقية عدم إفشاء متبادلة (NDA)، تقدّم Cyber Crucible حزمة أمان بائعين جاهزة تجيب عن مجالات الاستبيانات القياسية (SIG، CAIQ) وتحل محل تقرير SOC 2 في الحالات التي يبحث فيها المراجع عادةً عن تقرير من هذا النوع.

?? ?????? ?????? ??????????? ???????? ???

- حزمة جاهزة لأمان البائعين والثقة: البنية المعمارية، ومعالجة البيانات، والتشفير، وإدارة الوصول، والتطوير الآمن، والاستجابة للحوادث، واستمرارية الأعمال، والمواءمة التنظيمية، وربطها بأطر الضبط المعتمدة.
- ملخصات برامج من صفحة واحدة تخص الامتثال، والتدقيق، وحوكمة الذكاء الاصطناعي/دورة حياة تطوير البرمجيات (SDLC).
- شهادة تأمين، ونموذج W-9، ومعلومات مالية، متوفرة عند الطلب.
- البنود التعاقدية القياسية (SCC)، وتقييم مخاطر النقل (Transfer Risk Assessment)، واتفاقية معالجة البيانات (DPA)، متوفرة عند الطلب.

??????? ???? ????? ??????? ????

المستند	الموقع
اتفاقية مستوى الخدمة	cybercrucible.com/service-level-agreement
اتفاقية عدم الإفشاء المتبادلة	cybercrucible.com/mutualNDA
اتفاقية الخدمة الرئيسية وترخيص المستخدم النهائي (MSA & EULA)	cybercrucible.com/msa-and-eula
سياسة الخصوصية	cybercrucible.com/privacy-policy

يُقدّم كل ما يتجاوز الاتفاقيات العامة إلى المراجعين بموجب اتفاقية عدم إفشاء (NDA)، وفقًا لتدابير سرية معقولة.