

Wie unterstützt Cyber Crucible die NIS2-Pflichten für wesentliche und wichtige Einrichtungen?

Kurzantwort: Für eine Organisation, die im Rahmen von NIS2 als wesentliche oder wichtige Einrichtung eingestuft ist, unterstützt Cyber Crucible die erforderlichen Risikomanagementmaßnahmen – Endpunktschutz, Zugriffskontrolle, Verschlüsselung und Vorfallsbehandlung – und unterstützt die Erwartungen der Richtlinie an die Sicherheit der Lieferkette, da es keine Kundendaten erfasst und innerhalb der Grenzen der Einrichtung betrieben werden kann. Cyber Crucible unterstützt diese Pflichten; es zertifiziert sie nicht und übernimmt sie nicht.

Wie es NIS2-Maßnahmen unterstützt

- **Maßnahmen zum Cybersicherheitsrisikomanagement.** Autonome Endpunktprävention, MFA-gestützter Zugriff und Verschlüsselung entsprechen mehreren der grundlegenden Maßnahmen der Richtlinie.
- **Sicherheit der Lieferkette.** Als Anbieter, der keine Kundeninhalte erfasst und eine On-Premises-Bereitstellung anbietet, reduziert Cyber Crucible das Lieferkettenrisiko, das NIS2 von Einrichtungen zu managen verlangt, anstatt es zu erhöhen.
- **Unterstützung bei Vorfallsbehandlung und -meldung.** Ein dokumentierter Prozess zur Reaktion auf Sicherheitsverletzungen hilft der Einrichtung, die Fristen von NIS2 für Frühwarnungen und Benachrichtigungen einzuhalten.

Die ehrliche Grenze

Die NIS2-Pflichten liegen bei der wesentlichen oder wichtigen Einrichtung, nicht bei einem einzelnen Sicherheitstool. Die Umsetzung durch die Mitgliedstaaten fiel unterschiedlich aus: Bis 2026 hatten die meisten Staaten die Richtlinie in nationales Recht umgesetzt, während mehrere – darunter Frankreich, Irland, die Niederlande und Spanien – dies noch abschlossen. Cyber Crucible verfügt über keine NIS2-„Zertifizierung“; es stellt unterstützende Kontrollnachweise unter NDA bereit.

