

Bettet Cyber Crucible Bibliotheken oder Fremdcode von Drittanbietern ein?

Kurze Antwort: Nein. Kernel-Sensoren, Treiber und Genetic-AI-Verhaltensmodelle werden intern entwickelt. In die Software sind keine SDKs staatlich gesteuerter ausländischer Akteure, keine ungeprüften Bibliotheken von Drittanbietern und keine versteckten Telemetrie-Hooks eingebettet. Windows-Kernel-Treiber werden zur Zertifizierung im Rahmen des Windows Hardware Compatibility Program (WHCP) von Microsoft eingereicht.

Der technologische Wettbewerbsvorteil

Der interne Aufbau von Kernel-Sensoren und Verhaltensmodellen ist aufwendig und zeitintensiv. Die meisten Anbieter setzen stattdessen auf die Zusammenstellung vorhandener Komponenten. Genau an dieser Stelle entsteht in einem Sicherheitsprodukt das Risiko in der Lieferkette — und ausgerechnet das Tool mit den weitreichendsten Systemrechten ist dasjenige, bei dem eine ungeprüfte Abhängigkeit den größten Schaden anrichten kann.

Die Komponenten von Cyber Crucible sind proprietär und werden intern gepflegt, wodurch diese Art der Gefährdung von vornherein ausgeschlossen wird, anstatt sie lediglich zu verwalten.

Externe Validierung

Alle Windows-Kernel-Treiber durchlaufen interne Qualitätssicherungstests und werden zur Zertifizierung im Rahmen des Windows Hardware Compatibility Program (WHCP) von Microsoft eingereicht — eine unabhängige Validierung der Qualität und Manipulationssicherheit von Code, der auf Kernel-Ebene ausgeführt wird.

Keine versteckte Telemetrie

Es gibt keine versteckten Telemetrie-Hooks. Welche Daten die Software erfasst, ist dokumentiert, und die Kategorien, die niemals erfasst werden, sind ausdrücklich aufgeführt.