Was ist der Unterschied zwischen Systemtelemetrie und Kundendaten?

Kurze Antwort: Systemtelemetrie beschreibt, wie sich Software verhält — welcher Prozess welchen anderen gestartet hat, wie der Speicher aussieht, ob Ausführungsmuster anomal sind. Kundendaten sind die Inhalte, die Ihr Unternehmen erstellt und vorhält — Dateien, E-Mails, Datenbankeinträge, Zugangsdaten. Cyber Crucible analysiert Ersteres und erfasst niemals Letzteres.

Eine nützliche Betrachtungsweise

Telemetrie sind Metadaten über *Maschinenverhalten*. Inhalte sind die *Information selbst*.

Zu wissen, dass `Prozess A` `Prozess B` gestartet hat, der wiederum versucht hat, einen Browser-Zugangsdatenspeicher zu lesen und dabei Anzeichen einer In-Memory-Modifikation zeigte, genügt, um einen Angriff zu identifizieren. Zu lesen, was sich in diesem Zugangsdatenspeicher befand, ist nicht erforderlich — und Cyber Crucible tut dies nicht.

Was das praktisch bedeutet

- Die Verhaltensanalyse erfolgt beim Zugriff auf Identitäten, **ohne die Identitätsinformationen selbst zu verarbeiten**.
- Telemetrie, die bei Cloud-unterstützten Bereitstellungen den Endpunkt tatsächlich verlässt, beschränkt sich auf betriebliche Indikatoren für Health-Monitoring und Sicherheitsberichterstattung.
- Technische und verhaltensbezogene Metadaten werden nur dann als personenbezogene Daten behandelt, wenn sie eine Person direkt oder indirekt identifizieren können — in diesen Fällen werden Kennungen pseudonymisiert oder maskiert.

Kundenkontrolle

Telemetriequellen sind konfigurierbar. Organisationen können festlegen, welche Quellen erfasst werden, sodass keine unnötigen Informationen erhoben werden. Felder, die für die Bedrohungserkennung nicht essenziell sind, werden ausgeschlossen oder verworfen.

Revision #1
Created 2026-07-24 04:41:59 UTC by Dennis Underwood
Updated 2026-07-24 04:41:59 UTC by Dennis Underwood