Funktioniert Cyber Crucible zusammen mit anderen Cybersicherheits- und EDR-Tools?

Kurze Antwort: Ja. Cyber Crucible basiert auf eigenen, proprietären Sensoren und einer eigenen Verhaltensüberwachungstechnologie und läuft daher parallel zu praktisch jedem anderen Sicherheitsprodukt, ohne bestehende Tools zu beeinträchtigen.

Warum Kompatibilität kein Problem darstellt

Cyber Crucible ist nicht auf gemeinsam genutzte EDR-Hooks oder systemweite Integrationen angewiesen, auf die auch andere Sicherheitsanbieter zurückgreifen. Da der Erkennungs- und Überwachungsansatz, einschließlich der Methoden zur Verhaltenserfassung hinter FortressAI, von Grund auf individuell entwickelt wurde, konkurriert Cyber Crucible nicht um dieselben Systemressourcen und stört nicht die Hooks, die andere Endpoint-Protection-Tools verwenden. Durch dieses Design kann Cyber Crucible als zusätzliche Schutzebene fungieren, statt als Ersatz oder als störende Überlagerung. Die Lösung wurde bereits gemeinsam mit Produkten einer Vielzahl etablierter Sicherheitsanbieter eingesetzt, und in der Praxis zeigen sich in den meisten Umgebungen überhaupt keine Kompatibilitätsprobleme.

Wann Anpassungen erforderlich sind

Die seltene Situation, die zusätzliche Konfiguration erfordert, betrifft individuell entwickelte, intern erstellte Software eines Unternehmens. Gelegentlich zeigen diese selbst entwickelten Tools Verhaltensmuster, die den Aktivitäten ähneln, die Cyber Crucible erkennen soll, etwa schnelle Dateiänderungen oder ungewöhnliche Systeminteraktionen. In solchen Fällen ist die Lösung einfach: Eine Ausschlussregel kann hinzugefügt werden, damit Cyber Crucible das interne Tool als legitim erkennt. Dieser Ausschluss bleibt zuverlässig, solange die interne Software ordnungsgemäß signiert und unverändert bleibt, das heißt, solange sie weiterhin ihrem erwarteten, verifizierten Zustand entspricht. Sind diese Bedingungen erfüllt, funktioniert das Tool ohne fortlaufende Reibung

normal neben Cyber Crucible.

Was das für Sicherheitsteams bedeutet

Organisationen müssen ihren aktuellen Sicherheits-Stack nicht entfernen oder neu konfigurieren, um Cyber Crucible einzuführen. Die Lösung wurde entwickelt, um bestehende Schutzmaßnahmen zu ergänzen, indem sie eine dedizierte Ebene hinzufügt, die sich auf die Prävention von Ransomware, Datendiebstahl und Identitätsdiebstahl konzentriert, ohne die bereits vorhandenen Schutz-Tools in der Umgebung zu stören.

https://player.vimeo.com/video/1043463490?texttrack=de

Auf Vimeo ansehen · Untertitel: English, Français, Español, العربية

Revision #2
Created 2026-07-24 05:03:02 UTC by Dennis Underwood
Updated 2026-08-06 18:36:41 UTC by Dennis Underwood