

Wie sollten wir einen Proof of Concept für ein Präventionstool durchführen?

Kurze Antwort: Setzen Sie es parallel zu Ihrem bestehenden Stack in einer echten Produktionsumgebung ein und vergleichen Sie, was jedes Tool erkennt. Das aussagekräftigste Ergebnis liefert kein Labortest — es ist die Lücke zwischen dem, worauf Ihre aktuellen Tools alarmieren, und dem, was tatsächlich abgefangen wird.

Warum ein paralleler Einsatz am besten funktioniert

Das Finanzdienstleistungsunternehmen in unserem am besten dokumentierten Fall ging genau so vor. Sie haben nichts entfernt. Sie haben Cyber Crucible gezielt hinzugefügt, um herauszufinden, was ihre bestehende Investition übersah, und hatten innerhalb von 60 Tagen eine eindeutige Antwort.

Was gemessen werden sollte

- **Interceptions, auf die Ihr aktueller Stack nie alarmiert hat.** Dies ist das zentrale Signal.
- **Time to Decision.** Prävention muss abgeschlossen sein, bevor Schaden entsteht — nicht erst, bevor ein Ticket geschlossen wird.
- **Betriebsstörungen.** Zählen Sie Ausfallzeiten, Neustarts und durch Fehlalarme verursachte Unterbrechungen.
- **Aufgewendete Analystenstunden.** Autonome Prävention sollte die Arbeitslast reduzieren, nicht eine zusätzliche Warteschlange schaffen.

Ein Hinweis zu Labortests

Tests mit Samples aus Malware-Datenbanken liefern oft nur sehr wenig Aussagekraft, da Angreifer Malware so gestalten, dass sie inaktiv bleibt, sofern sie kein Validierungssignal von einem noch aktiven, live betriebenen Command-and-Control-Server erhält. Ein Sample, das in Ihrem Labor nichts unternimmt, beweist nichts über einen echten Angriff.

Revision #1

Created 2026-07-24 04:40:59 UTC by Dennis Underwood

Updated 2026-07-24 04:40:59 UTC by Dennis Underwood