

Warum erzeugt intentbasierte Prävention weniger Alarm-Rauschen als signaturbasierte Erkennung?

Kurze Antwort: Weil dabei eine engere Fragestellung gestellt wird. Signatur- und heuristische Tools schlagen Alarm, sobald etwas einem *bekannten schädlichen Muster ähnelt*, und überlassen es Menschen, die Spreu vom Weizen zu trennen. Intentbasierte Prävention fragt, ob ein bestimmtes Programm gerade jetzt an einem bekannten Einstiegspunkt für Datendiebstahl etwas Böses tut – eine Frage mit weitaus weniger mehrdeutigen Antworten.

“ Die gemessene Falsch-Positiv-Rate von Cyber Crucible finden Sie im bestehenden Artikel „**Haben Sie Fehlalarme? Wie hoch ist Ihre Fehlalarmrate?**“. Diese Seite erläutert den architektonischen Grund, warum sich das Rauschprofil unterscheidet.

Warum sich das Rauschprofil unterscheidet

Signatur- und heuristische Tools erzeugen Alarme, wenn etwas *einem bekannten schädlichen Muster ähnelt*, und verlassen sich anschließend auf manuelle Triage, um Echtes von Irrelevantem zu unterscheiden. Genau das führt in vielen Umgebungen zu über 100 Alarmen pro Endpunkt und Tag.

Die intentbasierte Bewertung stellt eine engere Frage: Tut dieses Programm gerade jetzt etwas Böses an einem bekannten Einstiegspunkt für Identitäts- oder Datendiebstahl? Diese Frage hat weitaus weniger mehrdeutige Antworten.

Was das operativ bedeutet

- Analysten müssen keinen Alarmen mit geringer Zuverlässigkeit nachjagen.

- Es ist keine YARA-Regel-Feinabstimmung oder manuelle Bedrohungssuche erforderlich, um das Rauschen beherrschbar zu halten.
- Da die Reaktion nur den betreffenden Prozess unterbricht, führt selbst eine fehlerhafte Intervention nicht zum Ausfall eines Systems.

Für aktuelle gemessene Werte in einer Umgebung wie der Ihren wenden Sie sich an Ihren Cyber-Crucible-Ansprechpartner – und lesen Sie den bestehenden Artikel „Haben Sie Fehlalarme?“ für Details auf Produktebene.

Revision #1

Created 2026-07-24 04:41:34 UTC by Dennis Underwood

Updated 2026-07-24 04:41:34 UTC by Dennis Underwood