

RUNBOOK

KI-gestützte Incident Response

Muster für die Erstreaktion: Log-Triage, Runbook-Erweiterung und Hypothesen-Bildung - plus die Punkte, an denen ein Mensch entscheiden muss.

Die ersten fünfzehn Minuten

Wenn ein Alert auslöst, ist die knappe Ressource nicht Intelligenz - es ist organisierte Aufmerksamkeit. KI verdient ihren Platz in der Incident Response, indem sie den Suchraum verdichtet: Sie liest die verrauschten Logs, korreliert die Timeline und entwirft Erklärungskandidaten, während die verantwortliche Person die Kontrolle über das behält, was tatsächlich geschieht.

01 Erst eindämmen, dann analysieren

Folgen Sie vor jeder KI-gestützten Analyse Ihrem Standard-Containment-Runbook - isolieren, sichern, benachrichtigen. Modellzeit ist billig; das Fenster, in dem Containment noch wirkt, nicht.

02 Logs durch das Modell triagieren

Speisen Sie die Logs des Alert-Fensters - bei sensiblem Kontext über selbst gehostete Inferenz - und verlangen Sie eine strukturierte Zusammenfassung: was sich änderte, was anomal ist, was wahrscheinlich Rauschen ist. Verifizieren Sie jede Aussage gegen die zitierten Rohzeilen.

03 Hypothesen generieren, gerankt

Verlangen Sie Ursachenkandidaten, geordnet nach Belegen in Ihren Daten, nicht nach generischer Wahrscheinlichkeit. Die Aufgabe des Modells ist das Aufzählen; Ihre ist das Falsifizieren.

04 Das Runbook erweitern

Passt der Vorfall zu einem bekannten Muster, lässt das Modell die relevanten Runbook-Schritte holen und mit beobachteten Werten füllen. Die verantwortliche Person führt aus - das Modell berührt die Produktion nicht.

05 Die Timeline laufend entwerfen

Lassen Sie das Modell die Incident-Timeline aus Ihren verifizierten Aktionen pflegen. Die Nachbesprechung startet dann mit einer schriftlichen Aufzeichnung, nicht aus dem Gedächtnis.

Wo der Mensch entscheidet - immer

- ☐ Das Deklarieren eines Incidents - Schweregrad und Umfang sind Verantwortungsentscheide, keine Textvervollständigung
- ☐ Jede Aktion auf Produktionssystemen - Restarts, Isolation, Rollbacks laufen durch menschliche Hände mit Änderungsnachweis

- ☐ Kunden- oder Behördenkommunikation - Formulierungen mit rechtlichem und vertraglichem Gewicht werden von Menschen geschrieben
- ☐ Eradikations- und Recovery-Schritte - ein Modell schlägt Reihenfolgen vor, eine verantwortliche Person bestätigt jede Vorbedingung vor der Ausführung
- ☐ Das Schliessen des Incidents - der finale Entscheid, dass Systeme wieder vertrauenswürdig sind, bleibt bei einer namentlichen Person

Wir betreiben unsere Security Operations auf Wazuh mit genau dieser Trennung: Detection und erste Entwürfe sind automatisiert, jede folgenschwere Aktion ist ein protokollierter menschlicher Entscheid.

Nach dem Incident

Die Timeline des Modells und Ihre verifizierten Aktionen werden zum Input der Nachbesprechung. Lassen Sie das Modell die Berichtsstruktur entwerfen - Fakten, Auswirkung, Faktoren, Prävention - und schreiben Sie um, bis es stimmt. Das Muster, das sich über Zeit auszahlt: Bestätigte Erkenntnisse fließen zurück in Detection-Regeln und Runbooks, sodass die nächste Reaktion weiter vorne beginnt als diese.

Dieses Dokument ist Teil der UHL-Ressourcen. Direkter Download und verwandte Arbeiten:
<https://uhl.cloud/de/resources/>

