Die Erkennung testen: Negativkontrollen statt grüner Dashboards

PRUEFEN. BELEGEN. NACHHALTEN.

Für einen eigenen SIEM-Erkennungsfall mit dokumentierter Logquelle, Regel und Bearbeitungsweg. Richtwert: 90 Minuten bei vorhandenen Testdaten; längere Regelintervalle und Datenlatenzen zusätzlich. Replay-Tests und echte Ereignisketten getrennt ausweisen.

Pruefbereich / Team:

Datum:

- [ ] **01 / Eine falsifizierbare Erkennungshypothese festlegen: Ereignis, Identität, Ergebnis, Zeitfenster und erwartete Alarmentscheidung.**

  Nachweis: Regelsteckbrief mit mindestens einem erwarteten Treffer und einem möglichst ähnlichen Nichttreffer.

- [ ] **02 / Pflichtfelder vom Quellereignis bis zur normalisierten Tabelle prüfen; fehlende oder falsch typisierte Werte sichtbar machen.**

  Nachweis: Verknüpfte Roh- und Normalereignisse mit Zeit, Ergebnis, stabiler Identitäts-ID und Testkennzeichen.

- [ ] **03 / Lookback, Ausführungsintervall und reale Ingestionsverzögerung gemeinsam gegen verpasste oder doppelte Ereignisse prüfen.**

  Nachweis: Zeitdiagramm und belegter Test am Zeitfensterrand; verspätete Daten ausdrücklich berücksichtigt.

- [ ] **04 / Eine harmlose Positivkontrolle über die echte Quelle erzeugen und bis zur zuständigen Bearbeitung verfolgen.**

  Nachweis: Zusammenhängende IDs und Zeitpunkte für Ereignis, Eingang, Regelmatch, Alarm, Routing und Annahme.

- [ ] **05 / Eine Negativkontrolle mit genau einer geänderten entscheidenden Eigenschaft auswerten; erwartete Nichttreffer vom Ausfall der Pipeline unterscheiden.**

  Nachweis: Versionierte Testpaare, Soll-Ist-Entscheidung und nachgewiesener Eingang beider Testereignisse.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 18

- [ ] **06 / Ausnahmen, Unterdrückung, Schwellwerte und Incident-Gruppierung auf verdeckte Treffer und unnötige Mehrfachalarme prüfen.**

  Nachweis: Regel- und Ausnahmestand sowie getrennte Nachweise für Match, Alert und angelegten beziehungsweise zugeordneten Incident.

- [ ] **07 / Ausfall einer dedizierten Testquelle sowie deaktivierte oder fehlerhafte Testregeln als Betriebsfehler erkennbar machen.**

  Nachweis: Gesonderter Health-Alarm mit Besitzer und Frist; ausbleibende Sicherheitsalarme werden nicht als Entwarnung gewertet.

- [ ] **08 / Die getestete Regelversion, Parser, Daten und Grenzen sichern und bei relevanten Änderungen erneut prüfen.**

  Nachweis: Reproduzierbarer Testbericht mit bekannten Blindstellen und ohne Zugangsdaten oder unnötige personenbezogene Inhalte.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Im isolierten Testarbeitsbereich ein freigegebenes synthetisches Ereignispaar für die Kopie einer Regel 'fehlgeschlagene Anmeldung des Testkontos' auswerten. Bei getrennten Test-IDs unterscheidet sich fachlich nur das Ergebnis: einmal fehlgeschlagen, einmal erfolgreich. Bestehen: Beide Ereignisse sind eingegangen, genau der Fehlerfall trifft und der Erfolgsfall nicht. Regelversion, Zeitfenster und Ausnahmen mit sichern; dieses Replay belegt nicht die echte Sensorstrecke.

GRENZEN UND VORAUSSETZUNGEN

Ein Query-Treffer ist noch kein zugestellter Alarm; ein Alarm ist noch kein bearbeiteter Incident. Synthetisch eingespielte Daten prüfen die vorgelagerten Sensoren nicht. Ein gesunder Connector beweist keine korrekte Regel. Erwartete Nichttreffer sind nur aussagekräftig, wenn die Testdaten nachweislich angekommen und vom geprüften Lauf erfasst worden sind.

PRIMAERQUELLEN / STAND 09.11.2026

OWASP: Logging Cheat Sheet - Verification
cheatsheetseries.owasp.org

Microsoft Learn: Scheduled analytics rules
learn.microsoft.com

Microsoft Learn: Monitor analytics rule health and integrity
learn.microsoft.com

Microsoft Learn: Enable Sentinel auditing and health monitoring
learn.microsoft.com

CISA und Partner: Best practices for event logging and threat detection
media.defense.gov