/ MAURISEC.DE

FIELD NOTES / CHECKLIST 10

Cloud-Logs, die im Vorfall tatsächlich helfen

PRUEFEN. BELEGEN. NACHHALTEN.

Anbieterübergreifende Prüfhilfe für Cloud- und Security-Teams. Erfassungsumfang, Datenquellen, Kosten und Verfügbarkeit sind je Dienst, Konfiguration und Vertrag gesondert zu prüfen.

Pruefbereich / Team:

Datum:

- [ ] **01 / Relevante Vorfallsfragen und Verantwortliche festlegen: Anmeldung, Rechteänderung, Schlüsselerstellung, Konfigurationsänderung und Zugriff auf schützenswerte Daten.**

  Nachweis: Priorisierte Erkennungsfälle mit benannter Datenquelle und Reaktionsweg.

- [ ] **02 / Management-/Audit-Logs und erforderliche Datenzugriffslogs getrennt prüfen; nicht voraussetzen, dass alle Ereignisarten standardmäßig erfasst werden.**

  Nachweis: Aktivierung, Geltungsbereich und Testereignis je kritischem Cloud-Dienst.

- [ ] **03 / Alle relevanten Konten, Projekte, Regionen und Dienste in die zentrale Erfassung aufnehmen.**

  Nachweis: Quelleninventar und Abgleich der erwarteten mit den tatsächlich eintreffenden Quellen.

- [ ] **04 / Identität, Aktion, Ressource, Ergebnis, Zeitstempel und geeignete Korrelationsmerkmale erhalten; Zeitzonen und Zeitformat normalisieren.**

  Nachweis: Durchgängig auswertbares Beispielereignis und überprüfte Zeitbasis.

- [ ] **05 / Logs zentral gegen unbemerkte Änderung und Löschung schützen; Zugriff auf Suche, Export und Konfiguration nach Aufgaben begrenzen.**

  Nachweis: Berechtigungstests, Aufbewahrungskonfiguration und Protokollierung von Änderungen am Logging.

- [ ] **06 / Aufbewahrung nach Untersuchungsbedarf und Datenschutz festlegen; benötigte Ereignisse über den festgelegten Zeitraum tatsächlich wiederfinden können.**

  Nachweis: Begründete Fristen, erfolgreiche historische Suche und getesteter Export.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 10

- [ ] **07 / Ausfall der Übertragung, ungewöhnlich lange Verzögerungen und deaktivierte Quellen erkennen und zuständigen Personen melden.**

  Nachweis: Kontrollierter Ausfalltest und bestätigter Alarm für eine fehlende Quelle.

- [ ] **08 / Erkennungsregeln mit ungefährlichen Testereignissen prüfen; Fehlalarme und nicht abgedeckte Varianten dokumentieren.**

  Nachweis: Vom Ereignis über die Warnung bis zur Bearbeitung belegte Testkette.

- [ ] **09 / Keine Passwörter, Access-Tokens oder unnötigen personenbezogenen Inhalte protokollieren; Fehlerpfade und Log-Injection berücksichtigen.**

  Nachweis: Stichprobenprüfung, Maskierung und Test ungültiger beziehungsweise manipulierter Eingaben.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Ein harmloses autorisiertes Testereignis auslösen und Quelle, Übertragung, Suchbarkeit und gegebenenfalls Alarmierung getrennt nachweisen.

GRENZEN UND VORAUSSETZUNGEN

Ein aktivierter Log-Dienst ist noch keine vollständige Sichtbarkeit oder wirksame Erkennung. Retention und Datentypen können kosten- oder lizenzabhängig sein. Automatische Sperren brauchen einen getesteten und zur Umgebung passenden Ablauf. Diese Checkliste legt keine pauschale gesetzliche Aufbewahrungsfrist fest.

PRIMAERQUELLEN / STAND 09.11.2026

Gemeinsame ACSC/CISA/NSA-Behördenempfehlung: Event Logging and Threat Detection
www.cyber.gov.au

CISA: Veröffentlichung der gemeinsamen Logging-Empfehlung
content.govdelivery.com

OWASP: Logging Cheat Sheet
cheatsheetseries.owasp.org