SKAFFON

Wir schaffen. Damit Sie mehr schaffen.

MUSTERBERICHT – FIKTIVE UMGEBUNG, KEIN KUNDENPROJEKT

Muster-Assessment Cloud Security

Beispielbericht einer technischen Cloud-Security-Prüfung: Scope, Methode, Befunde, Maßnahmen

Status	MUSTERBERICHT: fiktive Umgebung, kein Kundenprojekt
Stand	November 2026 (Version 1.0)
Herausgeber	SKAFFON GmbH, Grünwald bei München
Fiktiver Auftraggeber	Muster Maschinenbau GmbH
Umgebung (fiktiv)	AWS-Organisation mit vier Konten, ein Kubernetes-Cluster
Referenzen	CIS Benchmarks (Referenz-Regelwerk), BSI C5 (thematische Orientierung, keine Prüfung)

Musterbericht: fiktive Umgebung, kein Kundenprojekt. Alle Organisationen, Konten, Systeme, Befunde, Zahlen und Konfigurationsauszüge in diesem Dokument sind frei erfunden und dienen ausschließlich dazu, Aufbau, Tiefe und Einstufungslogik eines SKAFFON Cloud Security Assessments zu zeigen. Sie beschreiben keine reale Umgebung, keinen Kunden und kein tatsächliches Prüfergebnis. Es wurde keine reale Umgebung geprüft.

Muster-Assessment Cloud Security: Beispielbericht

Musterbericht: fiktive Umgebung, kein Kundenprojekt. Alle Organisationen, Konten, Systeme, Befunde, Zahlen und Konfigurationsauszüge in diesem Dokument sind frei erfunden und dienen ausschließlich dazu, Aufbau, Tiefe und Einstufungslogik eines SKAFFON Cloud Security Assessments zu zeigen. Sie beschreiben keine reale Umgebung, keinen Kunden und kein tatsächliches Prüfergebnis. Es wurde keine reale Umgebung geprüft.

1. Management Summary

Gegenstand des Musterberichts ist die **fiktive** „Muster Maschinenbau GmbH“ mit einer Cloud-Umgebung auf AWS (vier Konten in einer Organisation) und einem Kubernetes-Cluster. Der Bericht zeigt, wie ein Befundbericht aufgebaut ist: Eine Gesamteinschätzung, eine nach Einstufung sortierte Befundliste, je Befund Beleg, Wirkungsbetrachtung und Maßnahme sowie ein priorisierter Maßnahmenplan.

Im Beispiel ergeben sich **12 Befunde**: 1 kritisch, 3 hoch, 5 mittel, 3 niedrig (alle erfunden). Die Gesamtaussage des Beispiels lautet: Der kritische Befund (F-01) wäre sofort zu beheben. Die drei hohen Befunde betreffen Administratorzugänge und offene Verwaltungswege. Die mittleren Befunde betreffen vor allem Nachvollziehbarkeit, Backup-Schutz und fehlende organisationsweite Leitplanken.

2. Auftrag und Scope (fiktiv)

Punkt	Festlegung im Beispiel
Auftraggeber	Muster Maschinenbau GmbH (fiktiv)
Anlass	Vorbereitung auf eine Kundenanforderung zum Nachweis technischer Sicherheitsmaßnahmen (fiktiv)
Plattformen im Scope	AWS-Organisation mit vier Konten (Verwaltung, Log-Archiv, Produktion, Stage); ein Kubernetes-Cluster „muster-eks“ im Produktionskonto
Nicht im Scope	Anwendungscode, Inhalte der Daten, Endgeräte, Penetrationstest, Red-Team-Übung, Rechtsberatung
Zugriff	Lesend, nach Least Privilege, befristet vergeben; kein Zugriff auf Produktivdaten; Auswertung von Konfigurationen und Metadaten
Bedrohungsmodell (Kurzfassung)	Kritisch sind die Kundendatenbank und die Produktions-Pipeline. Betrachtete Angreifer: externe Opportunisten (Internet-Scans), Abfluss von Zugangsdaten, kompromittierte interne Zugänge
Prüfzeitraum	Musterangabe: zwei Wochen im November 2026 (fiktiv)

3. Vorgehen und Methodik

1. **Bedrohungsmodell.** Kritische Daten und Dienste, Zugriffswege, Annahmen zu Angreifern. Daraus folgt, welche Befunde für den Auftraggeber schwer wiegen.
2. **Erfassung.** Lesende Konfigurations- und Metadatenexporte je Konto; Auswertung mit einem Regelwerk. Wo sinnvoll, werden Cloud-Security-Posture-Management-Werkzeuge (CSPM) eingesetzt; Befunde werden manuell auf Plausibilität und Auswirkung geprüft.
3. **Prüfkatalog.** Standard-Prüfumfang von SKAFFON in den Bereichen IAM, Netz, Verschlüsselung und KMS, Logging, Fehlkonfiguration und Backup.
4. **Einstufung.** Nach dem SKAFFON-Schema (Abschnitt 3.2).
5. **Maßnahmenplan.** Priorisierung mit Abhängigkeiten und Aufwandseinschätzung.
6. **Nachprüfung.** Nach Umsetzung werden die Befunde erneut geprüft (im Musterbericht nicht dargestellt).

3.1 Regelwerke und Einordnung

- **CIS Benchmarks** des Center for Internet Security dienen als Referenz-Regelwerk der jeweiligen Plattform, zum Beispiel für AWS und für Kubernetes (AWS, Kubernetes). Welche Benchmark-Version gilt, wird im realen Bericht ausgewiesen. Im Musterbericht werden bewusst keine Kontrollnummern genannt, weil keine reale Umgebung gegen eine bestimmte Version geprüft wurde.
- **BSI C5 (Cloud Computing Compliance Criteria Catalogue)** des Bundesamts für Sicherheit in der Informationstechnik (BSI-Seite) richtet sich an Cloud-Anbieter und dient hier nur als thematische Orientierung für die Bereiche des Prüfkatalogs. Der Bericht ist **keine** C5-Prüfung und kein C5-Testat; die Aufteilung der Verantwortung zwischen Anbieter und Kunde bleibt zu beachten.
- **Kein Zertifikat.** Der Bericht bestätigt keine Konformität mit einer Norm.

3.2 Einstufungsschema

Das Schema ist eine praktische Einordnung, kein CVSS-Ersatz. Maßgeblich sind drei Faktoren: **Erreichbarkeit** (extern oder intern), **Schadensradius** (ein System oder ganzes Konto) und **vorhandene Gegenmaßnahmen**.

Stufe	Bedeutung	Behebung
Kritisch	Aus dem Internet ohne Besonderheiten ausnutzbar oder erlaubt vollständige Kontoübernahme	sofort
Hoch	Ausnutzbar mit niedrigem Aufwand oder durch einen kompromittierten internen Zugang mit großem Schadensradius	kurzfristig
Mittel	Erfordert zusätzliche Bedingungen oder hat begrenzte Auswirkung	im regulären Maßnahmenplan
Niedrig	Abweichung von Best Practice ohne direkten Angriffsweg	bei Gelegenheit

4. Befunde

4.1 Übersicht (alle Angaben fiktiv)

ID	Bereich	Einstufung	Befund	Aufwand
F-01	Fehlkonfiguration	Kritisch	Speicher-Bucket mit Datenbank-Exporten öffentlich lesbar	S
F-02	IAM	Hoch	Administrator-Benutzer mit langlebigem Zugangsschlüssel und ohne MFA	M
F-03	Netz	Hoch	SSH-Zugang aus dem offenen Internet auf Bastion-Host	M
F-04	Netz	Hoch	Kubernetes-API-Endpunkt öffentlich ohne Adressbeschränkung	M
F-05	Logging	Mittel	Audit-Logs nicht organisationsweit, nicht manipulationsgeschützt	M
F-06	Verschlüsselung und KMS	Mittel	Kundenverwaltete Schlüssel ohne Rotation und mit breiter Schlüsselrichtlinie	S
F-07	Backup	Mittel	Backups im selben Konto ohne Schutz vor Löschung	M
F-08	Fehlkonfiguration	Mittel	Instance Metadata Service Version 1 aktiv	S
F-09	IAM	Mittel	Keine Service Control Policies; keine Regionsbeschränkung	M
F-10	IAM	Niedrig	Ungenutzte Rollen und Benutzer	S
F-11	Verschlüsselung und KMS	Niedrig	Standardverschlüsselung für Volumes nicht erzwungen	S
F-12	Fehlkonfiguration	Niedrig	Uneinheitliche Ressourcen-Kennzeichnung	S

Aufwand: S = Stunden bis wenige Tage, M = einige Tage, L = Wochen; grobe Musterangabe, im realen Bericht je Umgebung geschätzt.

4.2 Befunddetails (alle Angaben fiktiv)

F-01: Speicher-Bucket mit Datenbank-Exporten öffentlich lesbar

Feld	Inhalt (fiktiv)
Bereich / Einstufung	Fehlkonfiguration / **Kritisch**
Befund	Ein S3-Bucket im Konto „prod“ enthält nächtliche Datenbank-Exporte. Die Bucket-Richtlinie erlaubt Lesezugriff für alle Principals (`"Principal": "*"`); Block Public Access ist auf Kontoebene nicht aktiviert.
Wirkungsbetrachtung	Erreichbarkeit: extern, ohne Anmeldung. Schadensradius: ein Datenbestand, vollständige Kundendaten. Vorhandene Gegenmaßnahmen: keine (kein Zugriffsprotokoll auf Objektebene aktiv).
Belegart	Bucket-Richtlinie (JSON-Export), Kontoeinstellung „S3 Block Public Access“ (Konfigurationsauszug)
Maßnahme	Sofort: Block Public Access auf Konto- und Bucket-Ebene aktivieren, Richtlinie auf definierte Rollen beschränken, Zugriffsprotokollierung einschalten. Danach prüfen, ob Zugriffe durch Dritte stattgefunden haben (Protokolle, soweit vorhanden) und den Vorfallprozess des Kunden anstoßen. Als IaC festschreiben.
Aufwand	S (Stunden bis wenige Tage)

F-02: Administrator-Benutzer mit langlebigem Zugangsschlüssel und ohne MFA

Feld	Inhalt (fiktiv)
Bereich / Einstufung	IAM / **Hoch**
Befund	Ein IAM-Benutzer mit `AdministratorAccess` besitzt einen Zugangsschlüssel, der seit mehr als 400 Tagen nicht rotiert wurde, und hat keine MFA-Registrierung.
Wirkungsbetrachtung	Erreichbarkeit: extern bei Schlüsselabfluss. Schadensradius: gesamtes Konto. Vorhandene Gegenmaßnahmen: keine MFA-Bedingung; Schlüssel nicht eingeschränkt auf Quell-Adressen.
Belegart	IAM Credential Report (CSV-Auszug), Richtlinienzuordnung des Benutzers
Maßnahme	Benutzer durch föderierte Anmeldung (IAM Identity Center oder Ihr Identitätsanbieter) und befristete Rollen ersetzen; Schlüssel deaktivieren und nach Prüfung der Verwendung löschen; MFA für alle menschlichen Administratoren erzwingen.
Aufwand	M (einige Tage)

F-03: SSH-Zugang aus dem offenen Internet auf Bastion-Host

Feld	Inhalt (fiktiv)
Bereich / Einstufung	Netz / **Hoch**
Befund	Eine Security Group erlaubt TCP/22 von `0.0.0.0/0` auf eine Bastion-Instanz, über die Administratoren auf interne Systeme zugreifen.
Wirkungsbetrachtung	Erreichbarkeit: extern. Schadensradius: Zugriff auf interne Verwaltungsnetze bei Kompromittierung. Vorhandene Gegenmaßnahmen: Schlüsselauthentifizierung; keine zentrale Protokollierung der Sitzungen.
Belegart	Security-Group-Export (JSON), Netzdiagramm
Maßnahme	Verwaltungszugang über Sitzungsdienst (zum Beispiel AWS Systems Manager Session Manager) ohne offene Ports; alternativ Quelladressen auf das Unternehmensnetz beschränken; Sitzungen protokollieren.
Aufwand	M (einige Tage)

F-04: Kubernetes-API-Endpunkt öffentlich ohne Adressbeschränkung

Feld	Inhalt (fiktiv)
Bereich / Einstufung	Netz / **Hoch**
Befund	Der Verwaltungs-Endpunkt des Kubernetes-Clusters „muster-eks“ ist öffentlich erreichbar; die zulässigen Quelladressen sind nicht eingeschränkt.
Wirkungsbetrachtung	Erreichbarkeit: extern (Authentifizierung erforderlich). Schadensradius: Cluster und darauf laufende Workloads. Vorhandene Gegenmaßnahmen: Authentifizierung über IAM; Kubernetes-RBAC vorhanden, aber breit (siehe F-02).
Belegart	Cluster-Konfiguration (Auszug), Endpunkt-Einstellungen
Maßnahme	Öffentlichen Zugriff auf bekannte Quelladressen beschränken oder deaktivieren und privaten Zugang über VPN beziehungsweise Bastion-Ersatz (F-03) nutzen.
Aufwand	M (einige Tage)

F-05: Audit-Logs nicht organisationsweit, nicht manipulationsgeschützt

Feld	Inhalt (fiktiv)
Bereich / Einstufung	Logging / **Mittel**
Befund	CloudTrail ist nur in zwei von vier Konten aktiv. Die Protokolldatei-Validierung ist ausgeschaltet; der Log-Bucket liegt im selben Konto wie die Workloads und hat keine Objektsperre.
Wirkungsbetrachtung	Erreichbarkeit: intern. Schadensradius: Nachvollziehbarkeit im gesamten Unternehmen. Vorhandene Gegenmaßnahmen: Log-Bucket versioniert.
Belegart	Trail-Konfiguration (Auszug), Bucket-Einstellungen
Maßnahme	Organisationsweiten Trail aus dem Verwaltungskonto einrichten, Protokolle in ein separates Log-Archiv-Konto mit Objektsperre schreiben, Validierung aktivieren, Alarme für Änderungen an Trail und Rollen definieren.
Aufwand	M (einige Tage)

F-06: Kundenverwaltete Schlüssel ohne Rotation und mit breiter Schlüsselrichtlinie

Feld	Inhalt (fiktiv)
Bereich / Einstufung	Verschlüsselung und KMS / **Mittel**
Befund	Drei kundenverwaltete KMS-Schlüssel haben die automatische Rotation deaktiviert. Die Schlüsselrichtlinie delegiert Verwaltung und Nutzung gemeinsam an alle IAM-Principals des Kontos.
Wirkungsbetrachtung	Erreichbarkeit: intern. Schadensradius: alle mit dem Schlüssel verschlüsselten Daten. Vorhandene Gegenmaßnahmen: Zugriff nur aus dem Konto.
Belegart	KMS-Schlüsselrichtlinien (JSON), Rotationsstatus je Schlüssel
Maßnahme	Rotation aktivieren; Schlüsselverwaltung und -nutzung auf getrennte Rollen aufteilen; Zugriffe auf Schlüssel protokollieren und auswerten.
Aufwand	S (Stunden bis wenige Tage)

F-07: Backups im selben Konto ohne Schutz vor Löschung

Feld	Inhalt (fiktiv)
Bereich / Einstufung	Backup / **Mittel**
Befund	Backups der Datenbanken liegen im Produktionskonto. Ein Backup-Tresor mit Sperre (Vault Lock) ist nicht eingerichtet; ein Restore-Test ist nicht dokumentiert.
Wirkungsbetrachtung	Erreichbarkeit: intern. Schadensradius: Datenverlust bei Kompromittierung des Kontos (inklusive Backups). Vorhandene Gegenmaßnahmen: Zeitgesteuerte Sicherungen vorhanden.
Belegart	Backup-Plan-Konfiguration, Tresor-Einstellungen, Rückfrage nach Restore-Protokoll
Maßnahme	Kopie in ein getrenntes Konto mit unveränderlicher Aufbewahrung; getrennte Zugangsdaten; wiederkehrender, dokumentierter Restore-Test mit gemessener Dauer.
Aufwand	M (einige Tage)

F-08: Instance Metadata Service Version 1 aktiv

Feld	Inhalt (fiktiv)
Bereich / Einstufung	Fehlkonfiguration / **Mittel**
Befund	Auf 14 von 22 Instanzen ist IMDSv1 zulässig. Damit lassen sich Rollen-Zugangsdaten über Schwachstellen wie Server-Side Request Forgery auslesen.
Wirkungsbetrachtung	Erreichbarkeit: intern/extern, abhängig von Anwendungsschwachstellen. Schadensradius: Rechte der Instanzrolle. Vorhandene Gegenmaßnahmen: Instanzrollen sind teilweise eng gefasst.
Belegart	Instanz-Metadatenoptionen (Export je Instanz)
Maßnahme	Auf IMDSv2 umstellen (Token erforderlich) und per Richtlinie erzwingen; Beispiel siehe Abschnitt 5.
Aufwand	S (Stunden bis wenige Tage)

F-09: Keine Service Control Policies; keine Regionsbeschränkung

Feld	Inhalt (fiktiv)
Bereich / Einstufung	IAM / **Mittel**
Befund	Die Organisation verwendet keine Service Control Policies. Ressourcen können in allen Regionen angelegt werden; Root-Anmeldung ist nicht überwacht.
Wirkungsbetrachtung	Erreichbarkeit: intern. Schadensradius: ganze Organisation. Vorhandene Gegenmaßnahmen: Konten sind getrennt nach Umgebung.
Belegart	Organisationsstruktur (Export), fehlende Richtlinien
Maßnahme	Leitplanken als Service Control Policies (nicht genutzte Regionen sperren, Änderungen an Log-Konfiguration verhindern, Root-Nutzung alarmieren), per Pipeline ausgerollt und zuerst im Testkonto geprüft.
Aufwand	M (einige Tage)

F-10: Ungenutzte Rollen und Benutzer

Feld	Inhalt (fiktiv)
Bereich / Einstufung	IAM / **Niedrig**
Befund	Fünf IAM-Rollen und drei Benutzer wurden seit mehr als 90 Tagen nicht verwendet.
Wirkungsbetrachtung	Erreichbarkeit: intern. Schadensradius: abhängig von zugewiesenen Rechten. Vorhandene Gegenmaßnahmen: keine Administratorrechte betroffen.
Belegart	IAM Credential Report, „Last accessed“-Informationen
Maßnahme	Nach Rücksprache mit den Verantwortlichen deaktivieren, nach Karenzzeit löschen; quartalsweisen Berechtigungsreview einführen.
Aufwand	S (Stunden bis wenige Tage)

F-11: Standardverschlüsselung für Volumes nicht erzwungen

Feld	Inhalt (fiktiv)
Bereich / Einstufung	Verschlüsselung und KMS / **Niedrig**
Befund	In der Stage-Umgebung existieren zwei unverschlüsselte EBS-Volumes; die kontoweite Standardverschlüsselung ist nicht aktiviert.
Wirkungsbetrachtung	Erreichbarkeit: intern. Schadensradius: ein System. Vorhandene Gegenmaßnahmen: keine Produktivdaten in Stage (laut Angabe des Betriebs).
Belegart	EBS-Volume-Liste (Export), Kontoeinstellung
Maßnahme	Standardverschlüsselung kontoweit aktivieren; bestehende Volumes per Snapshot-Kopie verschlüsseln.
Aufwand	S (Stunden bis wenige Tage)

F-12: Uneinheitliche Ressourcen-Kennzeichnung

Feld	Inhalt (fiktiv)
Bereich / Einstufung	Fehlkonfiguration / **Niedrig**
Befund	Etwa ein Drittel der Ressourcen trägt keine Kennzeichnung für Verantwortliche und Schutzbedarf. Dadurch ist die Zuordnung von Befunden und Kosten erschwert.
Wirkungsbetrachtung	Erreichbarkeit: intern. Schadensradius: kein direkter Angriffsweg. Vorhandene Gegenmaßnahmen: –.
Belegart	Ressourcenliste mit Kennzeichnungen (Export)
Maßnahme	Verbindlichen Kennzeichnungsstandard als Richtlinie in der IaC-Pipeline durchsetzen.
Aufwand	S (Stunden bis wenige Tage)

4.3 Positive Feststellungen (fiktiv)

- Produktions- und Stage-Umgebung liegen in getrennten Konten.
- Alle Datenbanken sind im Ruhezustand verschlüsselt.
- Infrastruktur wird überwiegend als Code verwaltet; Änderungen laufen über Code-Review.

5. Beispiel einer Maßnahme als Infrastructure as Code

Zu F-01 und F-08 liefert der reale Bericht reproduzierbare Änderungen. Beispiele (Terraform, Syntax gegen die Provider-Dokumentation vor Anwendung prüfen; die Ressourcennamen sind fiktiv):

```
# F-01: Öffentlichen Zugriff auf den Bucket sperren
resource "aws_s3_bucket_public_access_block" "exports" {
  bucket                  = aws_s3_bucket.db_exports.id
  block_public_acls       = true
  block_public_policy     = true
  ignore_public_acls      = true
  restrict_public_buckets = true
}

# F-08: IMDSv2 erzwingen (Auszug aus einer Launch-Template-Definition)
resource "aws_launch_template" "app" {
  # ...
  metadata_options {
    http_endpoint = "enabled"
    http_tokens   = "required"
  }
}
```

6. Belegarten

Jeder Befund wird mit einem nachvollziehbaren Beleg hinterlegt, sodass Ihr Team ihn selbst prüfen kann. Der Bericht enthält Auszüge (mit geschwärzten Konto-IDs und Schlüsseln) und verweist auf vollständige Exporte im Anhang.

Belegart	Beispiele
Konfigurationsauszug	Richtlinien- und Konfigurationsdokumente als JSON (Bucket-Richtlinie, Security Group, Schlüsselrichtlinie)
Bericht der Plattform	IAM Credential Report, „Last accessed“-Informationen, Cluster- und Trail-Einstellungen
Export mit Zeitstempel	Listen von Ressourcen und Einstellungen (Instanzen, Volumes, Kennzeichnungen)
Diagramm	Netz- und Konto-Struktur, Zugriffswege
Rückfrage / Interview	Dokumentierte Angaben des Betriebs, wo Konfiguration allein nichts aussagt (zum Beispiel Restore-Test)

7. Maßnahmenplan

Phase	Befunde	Abhängigkeiten
Sofort	F-01	Keine; Vorfallprüfung des Auftraggebers parallel anstoßen
Kurzfristig	F-02, F-03, F-04	F-04 benötigt den Ersatz-Zugangsweg aus F-03; F-02 benötigt Identitätsanbieter
Regulärer Plan	F-05, F-06, F-07, F-08, F-09	F-09 (Leitplanken) zuerst im Testkonto prüfen; F-05 vor F-09, damit Änderungen an der Protokollierung geschützt sind
Bei Gelegenheit	F-10, F-11, F-12	F-12 als Richtlinie in der IaC-Pipeline

8. Nächste Schritte

1. **Besprechung** der Befunde mit IT-Leitung und Betrieb; Klärung der Priorisierung entsprechend Schutzbedarf.
2. **Umsetzungsentscheidung:** Ihr Team setzt um, SKAFFON setzt um, oder gemeinsam. Änderungen laufen über Ihre Änderungsprozesse und IaC-Reviews.
3. **Umsetzung** der priorisierten Maßnahmen.

4. **Nachprüfung** der behobenen Befunde und Übergabe-Dokumentation für den Betrieb.

9. Abgrenzung

- Dieser Musterbericht ist **fiktiv**. Er enthält keine Informationen aus einem Kundenprojekt und keine realen Prüfergebnisse.
- Ein Assessment ist **kein Penetrationstest**, keine Red-Team-Übung und kein Gutachten oder Zertifikat für Dritte.
- Werkzeuge liefern Befunde. Bewertung und Behebung bleiben technische Arbeit mit Ihrem Team.
- Aufbau und Prüfumfang entsprechen der Leistungsbeschreibung auf skaffon.de/cybersecurity/cloud-security/.