keepbit

SIEM – Security Information & Event Management

Ihre 6-Schritte-Checkliste für mehr IT-Sicherheit

Angriffe erkennen, bevor sie Schaden anrichten – mit zentralem Monitoring

Sicherheit beginnt mit dem ersten Häkchen

Ein SIEM sammelt und analysiert sicherheitsrelevante Daten aus Ihrer IT-Landschaft.

So erkennen Sie Angriffe frühzeitig, erfüllen Compliance-Vorgaben und beschleunigen Reaktionszeiten.

Diese Checkliste hilft Ihnen, Ihre IT-Sicherheit praxisnah zu überprüfen:

- ✓ Sind alle relevanten Systeme ans SIEM angebunden?
- ✓ Werden Alarme regelmäßig überprüft und optimiert?
- ✓ Ist ein klarer Prozess für Incident Response definiert?

Gehen Sie die folgenden Punkte Schritt für Schritt durch und finden Sie heraus, wie gut Sie vorbereitet sind.

keepbit

1

Grundlagen schaffen

- Ziele für SIEM definiert (z. B. Angriffserkennung, Compliance, forensische Analysen)?
- Management-Commitment vorhanden (Budget, Betriebskonzept)?
- Rollen & Verantwortlichkeiten festgelegt (SIEM-Admin, Analysten, Incident-Responder)?

2

Status Quo ermitteln

- Datenquellen identifiziert (Server, Firewalls, Endpoints, Cloud)?
- Bestehende Monitoring- und Logging-Prozesse bewertet?
- Risiken durch fehlende oder unzureichende Protokollierung analysiert?

3

Planung & Konzeption

- Use Cases für Korrelation definiert (z. B. Brute Force, Malware-Ausbreitung)?
- Architektur geplant (On-Prem, Cloud, Hybrid)?
- Ressourcen (Speicher, Personal, Lizenzen) eingeplant?
- Playbooks für Incident Handling erstellt?

4

Umsetzung & Betrieb

- Relevante Systeme angebunden und Log-Sammlung eingerichtet?
- Korrelationen und Alarmierungsregeln implementiert?
- Dashboards und Reports erstellt?
- Analysten und Administratoren geschult?

5

Überwachung & Verbesserung

- SIEM-Use-Cases regelmäßig überprüft und optimiert?
- KPIs gemessen (z. B. Mean Time to Detect, Anzahl False Positives)?
- Lessons Learned aus Incidents integriert?
- Kontinuierlicher Verbesserungs-prozess etabliert?

6

Integration in SOC & Compliance

- Schnittstellen zu SOC oder SIEM-Partnern eingerichtet?
- Anforderungen aus NIS-2 und ISO 27001 erfüllt?
- Audit-Reports archiviert und auswertbar?
- Kontinuierliche Verbesserung dokumentiert?

keepbit

keepbit

Ihr nächster Schritt

Sie möchten wissen, wie viele dieser Punkte Ihr Unternehmen bereits erfüllt?

- Füllen Sie die Checkliste aus.
- Bringen Sie sie zum Erstgespräch mit.

So können wir gezielt auf Ihre Situation eingehen und konkrete Empfehlungen ableiten.

Kostenlosen Beratungstermin buchen

Kontakt keepbit IT Solution GmbH, E-Mail: info@keepbit.de, Telefon: +49 (0)821 450 444 0, www.keepbit.de