

SOC VOM MSSP ODER VOM HERSTELLER?

Die Wahl eines Security Operations Centers ist eine Entscheidung für mehrere Jahre. Diese Fragen helfen dabei, den passenden Partner zu finden.

- **Was passiert, wenn nachts ein Angriff erkannt wird?**
Wer bewertet den Vorfall? Wer wird informiert? Wird aktiv reagiert oder nur alarmiert?
- **Versteht der Anbieter das Geschäft oder nur die Technologie?**
Werden kritische Geschäftsprozesse, Produktionssysteme oder Spezialanwendungen berücksichtigt?
- **Können individuelle Anforderungen abgebildet werden?**
Sind zusätzliche Datenquellen, Custom Detections und branchenspezifische Anwendungsfälle möglich?
- **Gibt es einen festen Ansprechpartner?**
Wer kennt die Umgebung? Wer begleitet Reviews und strategische Entscheidungen?
- **Welche Kosten entstehen wirklich?**
Gibt es Limits für Logs oder Datenvolumen? Welche Zusatzkosten können später entstehen?
- **Wird die Sicherheitslage aktiv verbessert?**
Werden Schwachstellen adressiert und Empfehlungen zur Optimierung gegeben?
- **Welche Rolle spielt KI im SOC?**
Wird KI bereits produktiv eingesetzt? Gibt es eine nachvollziehbare Roadmap?

DIE WICHTIGSTEN TAKE-AWAYS



Nicht die Technologie entscheidet, sondern die Reaktion im Ernstfall.



Ein gutes SOC verbessert die Sicherheitslage kontinuierlich.



KI wird zum entscheidenden Faktor moderner Security Operations.

