cycura

Kontrolliert sicher im Security Operations Center

Die 5 größten Fallen bei der SOC-Wahl – und wie Sie Hoheit statt Abhängigkeit sicherstellen

Die Realität: Ihre Security ist wahrscheinlich weniger kontrolliert, als Sie denken

Viele Unternehmen investieren in externe SOC-Dienstleister – und verlieren dabei die Kontrolle über ihre eigene Sicherheit. Die Detection-Logik gehört dem Anbieter, die Playbooks sind undurchsichtig, im Ernstfall fehlt die Steuerbarkeit.

Was Sie in diesem Guide erwartet

- Die 5 strategischen Fallen bei der SOC-Wahl
- Warum Monitoring ohne Hoheit gefährlich ist
- Das Framework für ein kontrollierbares SOC-Modell
- Ein 15-Punkte-Selbstcheck zur Einschätzung Ihrer Situation

cycura

1

Die Kontrollverlust-Falle (Vendor Lock-in)

DIE LÜCKE

Nicht jeder Anbieter arbeitet im Kundenenvironment, Detection-Logik und Playbooks liegen dann oft ausschließlich beim Anbieter. In den Verträgen wird oft auch nicht die Übertragung von IP geregelt. Detection-Regeln, Use-Cases und Response-Playbooks bleiben somit Eigentum des Anbieters oder zumindest für sie, undokumentiert. Sie mieten die Sicherheit, besitzen sie aber nicht.

DAS KONKRETE RISIKO

Ein Wechsel des Anbieters dauert 6-12 Monate oder ist unmöglich, da Sie keine Dokumentation besitzen. Sie sind faktisch abhängig vom Anbieter, da ohne Dokumentation keine Kontinuität gewährleistet ist. Bei Vertragsende stehen Sie mit leeren Händen da.

WAS WIR IN ASSESSMENTS FINDEN

- Verträge ohne Klauseln zur Dokumentationsübergabe
- Playbooks als „Betriebsgeheimnis" des Anbieters
- Keine schriftliche Beschreibung der Detection-Regeln
- Fehlende Exit-Klauseln oder hohe Ablösesummen

PRÜFPFAD

Vertrag → Anhänge → IP-Rechte/Dokumentationspflichten → Exit-Klauseln

cycura

2

Die Kulturkluft

DIE LÜCKE

Fehlender Cultural Fit bei globalen SOC-Anbietern. Günstige Anbieter setzen stark auf Offshore-Teams (z.B. Indien). Unterschiedliche Kommunikationskulturen, Sprachbarrieren und Zeitverschiebungen führen zu Reibungsverlusten.

DAS KONKRETE RISIKO

Im Ernstfall entstehen durch Missverständnisse kritische Verzögerungen. Ein 15-Minuten-Incident wird zu einer Stunde, weil Kontext verloren geht. Eskalationen scheitern an kulturell unterschiedlichen Vorstellungen von Dringlichkeit und Verantwortung.

WAS WIR IN ASSESSMENTS FINDEN

- Ausschließliche Ticket-Kommunikation, keine direkten Sprachkanäle
- Strikte Arbeitsweise nach Anweisung ohne eigenständiges Denken außerhalb der Vorgaben
- Unterschiedliche Verständnisse von „kritisch" und „eskalationswürdig"
- Keine dedizierten Analysten, sondern rotierende Teams ohne Kontinuität

PRÜFPFAD

Testphase → Eskalations-Szenario simulieren → Sprachtest direkt mit den Analysten (nicht nur dem Sales-Team)

cycura

3

Die Referenz-Illusion

DIE LÜCKE

Referenzen im SOC-Kontext sind teilweise nicht repräsentativ. Kunden mit externem SOC Anbieter wollen aus Security-Gründen oft gar nicht als Referenz genannt werden. Gleichzeitig zeigen Anbieter natürlich nur Erfolgsgeschichten. Das Bild ist zwangsläufig verzerrt.

DAS KONKRETE RISIKO

Sie kaufen die Katze im Sack. Der Anbieter zeigt Ihnen tolle Referenzen, aber im Ernstfall reagiert er langsam oder unprofessionell. Sie erfahren erst bei Ihrem eigenen Ransomware-Angriff, dass der Anbieter überfordert ist – und haben keine Alternative mehr.

WAS WIR IN ASSESSMENTS FINDEN

- Referenzen ohne Incident-Details oder MTTR-Angaben
- Keine transparenten Statistiken über reale Reaktionszeiten
- Nur Verfügbarkeits-SLAs (99,9%), aber keine Reaktions-SLAs bei echten Angriffen

PRÜFPFAD

Referenzgespräche → Gezielte Fragen nach Incidents der letzten 6 Monate → Anforderung realer MTTR-Statistiken (Median, nicht Durchschnitt)

cycura

4

Die Priorisierungsfalle

DIE LÜCKE

Der Anbieter ist zu groß für Sie oder fokussiert sich auf andere Branchen. Große SOC-Anbieter priorisieren ihre größten Kunden. Mittelstandskunden erhalten bei großen Anbietern oft nicht die Priorisierung, die im Ernstfall erforderlich ist.

DAS KONKRETE RISIKO

Während Sie unter einem aktiven Ransomware-Angriff stehen, arbeitet das erfahrene Senior-Team am großen Kunden. Sie erhalten nur Junior-Analysten. Ihr Business steht still, während Ihr Anbieter Sie nicht priorisiert.

WAS WIR IN ASSESSMENTS FINDEN

- „Shared Resources" ohne garantierte dedizierte Anteile
- SLA ohne Priorisierungs-Garantie oder Ressourcen-Zuordnung
- Anbieter mit 80% Enterprise-Kunden bei Mittelstand-Kunden
- Keine Eskalationsrechte zu Senior-Analysten im Vertrag verankert

PRÜFPFAD

Vertrag → SLA → Priorisierungsklauseln → Ressourcen-Garantie (dedicated vs. shared) → Eskalationsrechte

cycura

5

Die Template-Falle

DIE LÜCKE

Der Anbieter arbeitet ausschließlich mit festen Templates und Standard-Use-Cases (z.B. nur Windows, keine OT). Ihre spezifische Infrastruktur, Branchenrisiken und Legacy-Systeme werden nicht berücksichtigt.

DAS KONKRETE RISIKO

Spezifische Angriffe auf Ihre Branche (z.B. OT-Umgebung, spezielle ERP-Systeme) werden nicht erkannt. Der SOC meldet grün, während ein gezielter Angriff über Ihre spezifischen Schwachstellen läuft. Sie haben falsche Sicherheit und erfahren den Schaden erst durch Dritte.

WAS WIR IN ASSESSMENTS FINDEN

- Identische Detection-Regeln für alle Kunden (Copy-Paste)
- Keine Anpassung an branchenspezifische Threats (Healthcare, Manufacturing, Finance)
- Fehlende Custom-Use-Cases für Legacy-Systeme oder spezielle Applikationen
- Keine regelmäßige Anpassung der Detection an Ihre sich verändernde Umgebung

PRÜFPFAD

Onboarding-Dokumentation → Liste implementierter Use-Cases → Abgleich mit Ihren spezifischen Risiken (OT, IoT, Legacy) → Testangriffe auf spezifische Systeme

cycura

Das Problem: Security ohne Kontrolle

Ebene 1: Fehlende Hoheit

Sie haben einen SOC-Vertrag, aber keine Hoheit über Detection-Logik, Playbooks und Daten. Der Anbieter entscheidet, was wichtig ist.

Ebene 2: Fehlende Transparenz

Kein Überblick über reale Reaktionszeiten, keine Einsicht in Analysten-Qualifikation, keine Nachvollziehbarkeit bei Incidents.

Ebene 3: Fehlende Steuerbarkeit

Im Ernstfall können Sie nicht eingreifen, priorisieren oder eskalieren. Sie sind abhängig von fremden Prozessen.

cycura

Der SOC-Reifegrad-Check

Stufe	Beschreibung
1 Ad-hoc	Kein SOC oder reaktiver Einkauf ohne Konzept. „Wir haben einen Vertrag."
2 Definiert	Grundlegendes Monitoring aktiv, aber Lücken bei Kontrolle und Transparenz.
3 Gesteuert	Systematische SOC-Prozesse, aber keine kontinuierliche Überprüfung der Anbieterleistung.
4 Optimierend	Kontrolliertes Modell mit klaren Metriken (MTTR, Qualität), regelmäßigen Reviews und Hoheit über Detection.
5 Exzellent	Vollständige Hoheit, proaktive Anpassung, Integration interner und externer Ressourcen, risikobasierte Steuerung.

> **Die gute Nachricht:** Die meisten Unternehmen befinden sich auf Stufe 2 oder 3 – und können mit gezielten Maßnahmen innerhalb von 3-6 Monaten Stufe 4 erreichen.

Wo stehen Sie? – 5 Fragen zum Selbstcheck (Ja/Nein)

1. Können Sie jederzeit sagen, welche Detection-Regeln bei Ihrem Anbieter aktiv sind?
2. Wissen Sie, wer bei einem kritischen Incident konkret handelt (Name, Rolle)?
3. Haben Sie alle Playbooks und Response-Pläne in Ihrem Besitz?
4. Können Sie einen Incident bei Ihrem Anbieter priorisieren oder eskalieren?
5. Könnten Sie den Anbieter innerhalb von 30 Tagen wechseln, ohne Sicherheitslücken zu reißen?

cycura

Der 15-Punkte Risiko-Check (bei bestehendem SOC)

Beantworten Sie die folgenden Fragen mit Ja oder Nein. Jedes „Nein" ist ein potenzielles Risiko.

Kategorie: Hoheit & Kontrolle

1. Haben Sie vollständige Dokumentation aller Detection-Regeln in Ihrem Besitz?
2. Können Sie ohne Zustimmung des Anbieters die Detection-Logik ändern oder ergänzen?
3. Sind alle Incident-Response-Playbooks Ihr Eigentum und nachvollziehbar?
4. Gibt es eine definierte Exit-Strategie mit vollständiger Datenübergabe?
5. Können Sie den Anbieter technisch und organisatorisch innerhalb von 60 Tagen ersetzen?

cycura

Der 15-Punkte Risiko-Check (Fortsetzung)

Kategorie: Transparenz & Qualität

6. Wissen Sie jederzeit, welcher Analyst bei Ihrem Anbieter für Ihr Unternehmen zuständig ist?
7. Erhalten Sie transparente Reports über reale MTTR (Mean Time to Response) bei Incidents?
8. Haben Sie Einblick in die Qualifikation und Zertifizierung der Analysten?
9. Werden alle Incidents mit ausreichend Kontext dokumentiert (nicht nur „Alert closed")?
10. Wird die Detection-Qualität regelmäßig (mindestens vierteljährlich) an Ihre Risiken angepasst?

Kategorie: Reaktionsfähigkeit & Steuerung

11. Können Sie im Ernstfall direkt mit dem Analysten sprechen (nicht nur per Ticket)?
12. Gibt es garantierte Reaktionszeiten für kritische Incidents (nicht nur „best effort")?
13. Sind Eskalationswege zu Ihrem internen Team klar definiert und getestet?
14. Passt der kulturelle und sprachliche Background des SOC-Teams zu Ihrem Unternehmen?
15. Sind Sie als Kunde bei Ihrem Anbieter priorisiert (dedicated Ressourcen) oder Shared Resource?

cycura

Auswertung des 15-Punkte Risiko-Checks

Nein-Antworten	Risikostufe	Empfohlene Maßnahmen
0-2	Niedrig	Kontinuierliche Verbesserung, Monitoring ausbauen
3-5	Mittel	Quick Wins umsetzen, Prioritäten setzen
6-9	Hoch	Sofortige Maßnahmen erforderlich, Vertrag prüfen
10-15	Kritisch	Dringender Handlungsbedarf, professionelles Assessment buchen

Mehr als 3x „Nein"? Ihr SOC hat signifikante Risiken. Wir helfen Ihnen, systematisch Kontrolle zurückzugewinnen. **www.cycura.de/termin**

cycura

Impressum

cycura GmbH

Ihr Spezialist für Microsoft-Security

Kontakt:

E-Mail: info@cycura.de

Web: www.cycura.de

Handelsregister: Amtsgericht Göttingen HRB 206706

USt-IdNr.: DE354593485

Bereit, Ihre Risiken zu kennen?www.cycura.de/termin