sure[secure]
your security operations center

secure mag

SOC 2026

Zwischen AI-Debatte und Betriebsrealität

Effizienz als Betriebsmodell

Security Operations Center stehen im Jahr 2026 unter einem doppelten Druck. Auf der einen Seite professionalisieren sich Angreifer weiter, arbeiten arbeitsteilig, automatisiert und skalierbar und auf der anderen Seite bleiben Budgets begrenzt und der Fachkräftemangel - insbesondere bei spezialisierten Sicherheitsrollen - ein strukturelles Problem. Unternehmen sehen sich daher mit der Frage konfrontiert, wie sie ihre Sicherheitsfähigkeit erhöhen können, ohne ihre Organisation dauerhaft zu überlasten.

In diesem Kontext wird Effizienz zum dominierenden Schlagwort. Effizienz soll die Antwort sein auf steigende Alert-Zahlen, komplexere IT-Landschaften und 24x7-Anforderungen. Mit der wachsenden Diskussion um künstliche Intelligenz hat sich die Debatte zusätzlich verschoben, denn AI wird häufig als Beschleuniger oder gar als Lösung für strukturelle Engpässe dargestellt. Gleichzeitig wächst der Markt für Security-Services stark, die operative Entlastung versprechen.

Doch zwischen technologischem Fortschritt, Marktangeboten und realer Wirksamkeit besteht eine Lücke. Effizienz im SOC ist kein isolierter Effekt einzelner Technologien, sondern das Ergebnis eines durchdachten Zusammenspiels aus Detection-Qualität, klar definierten Rollen, standardisierten Prozessen, gezielter Automatisierung und messbarer Steuerung. AI kann dieses System unterstützen, ersetzt jedoch weder organisatorische Klarheit noch operative Verantwortung.

Hier werden daher drei zentrale Fragen untersucht: Wie entsteht Effizienz im SOC tatsächlich? Welche Rolle spielt AI realistisch betrachtet? Und wie können Unternehmen in einem zunehmend intransparentem SOC-Markt noch Entscheidungen treffen?

Ziel ist es, Security Operations nicht als Produkt oder Tool-Stack zu betrachten, sondern als Betriebsmodell.

Foto: Salih Ergün, Head of SOC Analysis, suresecure GmbH

Warum Effizienz 2026 zur Kernfrage wird

Die ENISA Threat Landscape 2025 beschreibt eine zunehmende Professionalisierung von Angreifergruppen. Kampagnen werden arbeitsteilig organisiert, automatisierte Werkzeuge reduzieren Aufwand und erhöhen Skalierbarkeit. Gleichzeitig werden Angriffe nicht zwingend spektakulärer, sondern systematischer und dauerhafter.

Das World Economic Forum betont im Global Cybersecurity Outlook 2025 die zunehmende wirtschaftliche Asymmetrie zwischen Angreifern und Verteidigern. Während Angreifer ihre Prozesse industrialisieren, stehen Verteidiger unter Budgetdruck.

Parallel dazu dokumentiert die ISC Workforce Study 2025 eine weiterhin erhebliche globale Lücke an qualifizierten Sicherheitsfachkräften. Besonders betroffen sind spezialisierte Rollen wie Incident Response, Security Engineering und Cloud Security.

Das bedeutet:

Mehr Angriffe.

Mehr Komplexität.

Nicht mehr Personal.

Effizienz ist damit keine Optimierung, sondern eine Überlebensfrage.

Effizienz entsteht durch Architektur

Effizienz im Security Operations Center wird derzeit häufig mit AI gleichgesetzt, aber diese Gleichsetzung greift zu kurz. Denn die Automatisierung im SOC ist kein neues Phänomen. Regelbasierte Korrelation, Playbooks und SOAR-Workflows existieren seit Jahren. Die aktuelle AI-Debatte fügt lediglich eine neue Ebene hinzu, insbesondere bei Kontextualisierung und kognitiver Unterstützung. Sie ersetzt aber nicht die strukturellen Grundlagen effizienter Security Operations.

Effizienz im SOC bedeutet nicht „schnell reagieren“, sondern eine durchgängig optimierte Incident-Kette: erkennen, zuweisen, reagieren und eindämmen, und das mit minimalem Reibungsverlust.

Ob diese Kette funktioniert, lässt sich an drei Kennzahlen ablesen: MTTD (Mean Time to Detect), MTTA (Mean Time to Assign) und MTTR (Mean Time to Respond/Resolve).

Diese KPIs sind keine Report-Zahlen, sondern operative Steuerungsinstrumente.

MTTD - Geschwindigkeit der Sichtbarkeit

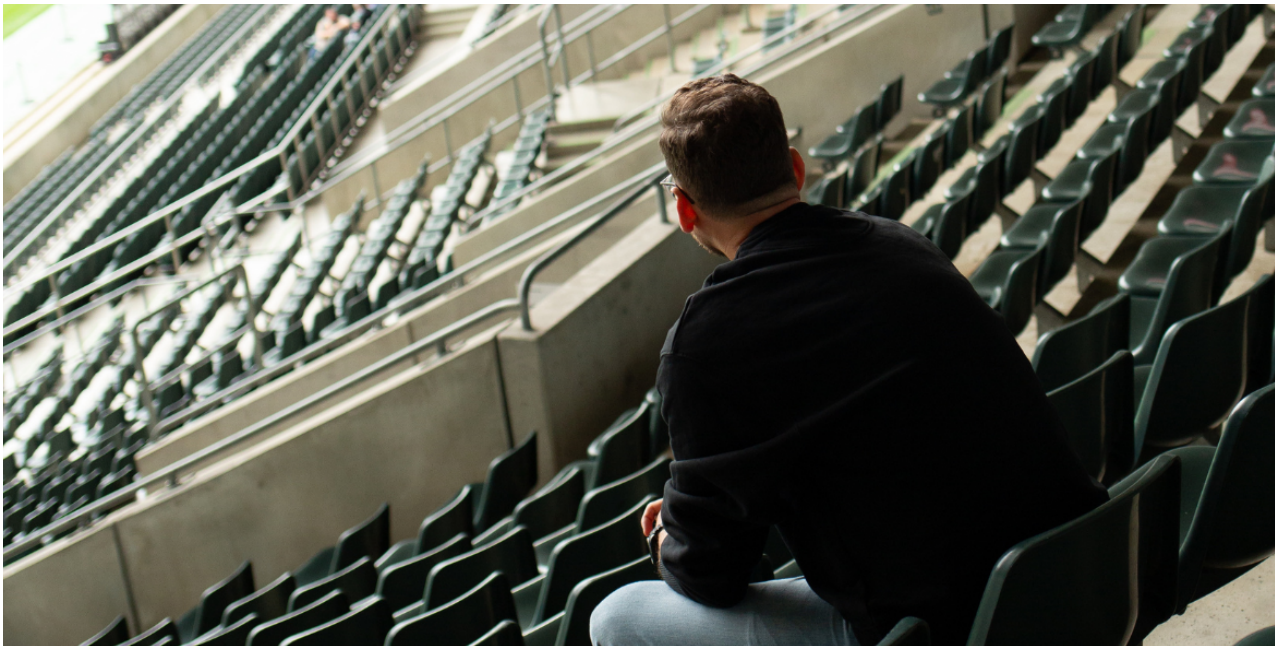
MTTD misst die Zeitspanne zwischen dem Eintritt eines Vorfalls und seiner Erkennung. In Marktvergleichen liegt die Erkennungszeit bei manuellen Prozessen häufig im Bereich von 30 bis 120 Minuten bei hochpriorisierten Fällen. In weniger reifen Umgebungen kann sie deutlich darüber liegen.

In automatisierten Umgebungen reduziert sich diese Zeit typischerweise auf 1 bis 10 Minuten. Das entspricht, abhängig vom Ausgangswert, einer Reduktion um häufig über 80 bis 90 Prozent.

Der Effekt entsteht nicht allein durch AI, sondern durch:

- automatisierte Priorisierung
- regelbasiertes Enrichment
- sofortiges Routing
- Reduktion manueller Vorvalidierung

Wichtig ist: Ein niedriger MTTD-Wert ist nur dann sinnvoll, wenn er nach Severity differenziert wird. Ein globaler Durchschnitt verschleiert strukturelle Unterschiede zwischen kritischen und mittleren Fällen.



MTTA - Wo Effizienz organisatorisch gewonnen wird

MTTA misst die Zeit zwischen Erkennung und Zuweisung eines Vorfalls. Diese Kennzahl wird häufig unterschätzt, obwohl sie zentral für operative Stabilität ist.

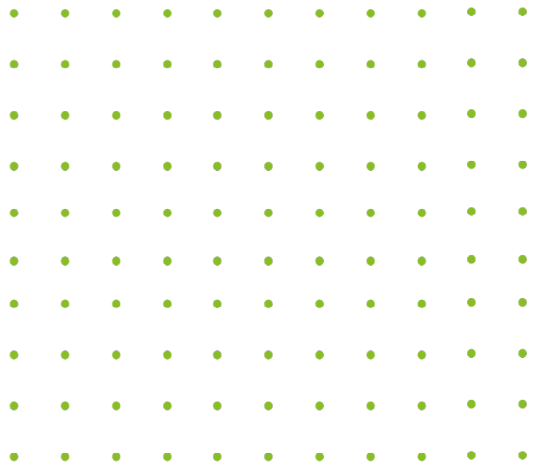
In manuellen Modellen liegt die Zuweisung bei kritischen Vorfällen häufig zwischen 10 und 60 Minuten. In automatisierten Routing-Strukturen kann dieser Schritt in weniger als fünf Minuten, teilweise sogar in unter einer Minute erfolgen.

Das bedeutet: Bereits vor Beginn der eigentlichen Bearbeitung kann Automatisierung den Zeitverlust um mehr als 80 Prozent reduzieren.

Ein hoher MTTA-Wert weist selten auf technische Schwächen hin. Meist sind es organisatorische Ursachen:

- Queue-Überlastung
- fehlende Eskalationslogik
- unklare Zuständigkeiten
- manuelle Klassifikation

Effizienz im SOC beginnt daher nicht mit AI, sondern mit Prozessklarheit.



MTTR - Die entscheidende Wirksamkeitskennzahl

MTTR misst die Zeit von der Erkennung bis zur Eindämmung oder vollständigen Reaktion. Hier entscheidet sich, ob ein Vorfall kontrolliert bleibt oder eskaliert.

Im Marktvergleich liegen manuelle Reaktionszeiten bei hochpriorisierten Vorfällen häufig im Bereich von mehreren Stunden. Bei mittleren Fällen sind vier bis zwölf Stunden keine Seltenheit.

Automatisierte Workflows können standardisierbare Fälle, etwa IOC-basierte Blockierungen oder klar definierte Policy-Verstöße, in wenigen Minuten eindämmen. In diesen Szenarien sind Reduktionen von deutlich über 80 Prozent gegenüber rein manuellen Prozessen realistisch.

Gleichzeitig bleibt ein erheblicher Anteil komplexer Vorfälle bewusst manuell. Hypothesengetriebene Analysen, geschäftskritische Entscheidungen oder forensische Bewertungen lassen sich nicht vollständig automatisieren. Effizienz entsteht daher nicht durch vollständige Automatisierung, sondern durch klare Trennung:

Was ist standardisierbar, und was erfordert menschliche Bewertung?

MTTD, MTTA und MTTR wirken nur im Zusammenspiel. So verliert z. B. eine schnelle Erkennung an Bedeutung, wenn die Zuweisung verzögert ist.

Automatisierung - mit oder ohne AI - reduziert insbesondere Wartezeiten und Reibungsverluste. In stark standardisierbaren Fällen können Reaktionsketten um mehr als 80 bis 90 Prozent beschleunigt werden. In komplexen Szenarien bleibt menschliche Expertise der limitierende, aber notwendige Faktor. Die zentrale Erkenntnis für 2026 lautet daher:

Effizienz entsteht nicht durch Technologie allein, sondern durch das Zusammenspiel aus Prozessreife, klaren Zuständigkeiten und gezielter Automatisierung. AI kann diese Kette beschleunigen. Sie ersetzt sie jedoch nicht.

Rollen und Verantwortlichkeiten im SOC 2026

Die Diskussion über Security Operations wird oftmals technikzentriert geführt. SIEM, SOAR, XDR oder AI: Die Debatte dreht sich um Plattformen, Features und Integrationen. Doch 2026 zeigt sich deutlicher denn je: Die Wirksamkeit eines SOC wird nicht durch den Tool-Stack bestimmt, sondern durch das Rollenmodell dahinter.

Der anhaltende Fachkräftemangel, dokumentiert in der ISC-Workforce-Study 2025, verschärft diesen Befund. Das Problem ist nicht nur die Anzahl verfügbarer Fachkräfte, sondern die zunehmende Spezialisierung der erforderlichen Kompetenzen. Detection Engineering, Incident Response, Plattformarchitektur und Automatisierung sind eigenständige Disziplinen geworden.

Gleichzeitig professionalisieren sich Angreifer weiter und arbeiten stark kampagnenorientiert, wie die ENISA Threat Landscape 2025 beschreibt. Diese Professionalisierung auf der Angriffsseite zwingt auch Verteidigungsstrukturen zu höherer Spezialisierung und klarer Verantwortungszuweisung.

Ein SOC 2026 ist daher kein homogenes Analystenteam. Es ist ein arbeitsteiliges System, in dem jede Rolle eine klar definierten Kernverantwortung trägt.

Die folgende Übersicht beschreibt die zentralen Rollen eines modernen SOC im Jahr 2026 inklusive ihrer Kernverantwortung sowie der spezifischen Herausforderungen, die sich aus technologischer Entwicklung, Marktbedingungen und regulatorischen Anforderungen ergeben.

Rolle	Definition	Kernverantwortung	Herausforderung 2026
Customer Success Manager	Strategische Schnittstelle im Service zwischen Kunde und SOC-Betrieb	■ KPI-Transparenz ■ Service-Reviews ■ Eskalationsmanagement ■ Roadmap-Abstimmung	■ Erwartungsmanagement zwischen Marketingversprechen und operativer Realität ■ Nachweis echter Wirksamkeit
Transition Manager	Verantwortlich für strukturierte und effiziente SOC-Onboardings	■ Migrationsplanung ■ Log-Onboarding ■ Prozessharmonisierung ■ Eskalationsdefinition ■ Go-Live-Management	■ Vermeidung von Detection-Lücken während Übergangsphasen ■ Wissensverlust bei Anbieterwechsel ■ Saubere Verantwortungsabgrenzung
SOC-Analyst	Operativer Kern des SOC: Monitoring, Triage, Analyse und Eskalation	■ Alert-Klassifikation und Priorisierung ■ Anwendung von Playbooks ■ Dokumentation ■ Eskalation an IR oder Engineering	■ Alert-Noise ■ AI-Assistenz kritisch bewerten („charming AI“) ■ steigende Tool-Komplexität

Rolle	Definition	Kernverantwortung	Herausforderung 2026
Incident Response Analyst	Verantwortlich für Analyse, Behebung und Aufarbeitung von Sicherheitsvorfällen	■ Incident-Scoping ■ Containment-Entscheidungen ■ Koordination mit IT/Management ■ Forensik-Grundlagen ■ Post-Incident-Analyse	■ Schnellere Angriffsbewegungen ■ Entscheidungsdruck bei Betriebsunterbrechungen ■ Dokumentationsanforderungen (Audit/Regulatorik)
Detection Engineer	Entwickelt und pflegt Detection-Logik als „Produkt“ des SOC	■ Entwicklung, Testing, Tuning und Versionierung von Detection Rules ■ Reduktion von False Positives; Coverage-Management	■ Komplexere Angriffsmodelle ■ Steigende Erwartung an Präzision bei gleichbleibendem Ressourcenstand
DevOps Engineer (Security Platform)	Stellt Stabilität, Skalierbarkeit und Automatisierbarkeit der Security-Plattform sicher	■ CI/CD für Detection & Playbooks ■ Infrastructure as Code ■ Performance-Optimierung	■ Tool-Fragmentierung ■ Steigende Datenmengen ■ Kostendruck bei Cloud-basierten Plattformen
Platform Engineer (SIEM/Data)	Verantwortlich für Datenqualität und technische Integrität der Plattform	■ Log-Normalisierung ■ Parser-Qualität ■ Latenzüberwachung ■ Retention-Strategie ■ Datenintegrität	■ Wachsende Datenquellen (SaaS, OT, Cloud) ■ Sicherstellung konsistenter Telemetrie
Support Engineer	Technischer Support für Plattformen, Integrationen und Security-Komponenten	■ Fehleranalyse ■ Störungsbehebung ■ Schnittstellenprüfung ■ Koordination mit Herstellern	■ Schnellere Release-Zyklen ■ Abhängigkeit von Drittanbieter ■ Minimierung von Downtime
System Engineer	Implementiert und betreibt Security-Komponenten wie EDR, Firewall, IAM	■ Deployment, Konfigurationshärtung ■ Policy-Management ■ Systemintegration	■ Fehlkonfigurationen als Hauptursache für Detection-Lücken ■ Zunehmende Hybrid- und Multi-Cloud-Umgebungen
SOAR & SIEM Engineer	Verantwortlich für Orchestrierung, Automatisierung und Plattformintegration	■ Playbook-Automatisierung ■ API-Integration ■ Workflow-Design ■ Auditierbarkeit ■ Performance-Tuning	■ Balance zwischen Automatisierung und Kontrolle ■ Skalierung ohne Fehler-Multiplikation ■ AI-Integration sinnvoll einordnen

PODCAST

CYBER SECURITY Basement

In unserem Podcast spricht Michael Döhmen über spannende Themen aus dem Bereich Cybersecurity. Dabei legen wir großen Wert auf Objektivität und verzichten auf übertriebenes Marketing oder „Feature-Fucking“. Stattdessen setzen wir auf einen seriösen, authentischen und ehrlichen Austausch zwischen Theorie und Praxis.

Jetzt reinhören

Spotify

Apple Podcast

YouTube Music

amazon music

und noch mehr...

AI im SOC 2026. Realität statt Autonomie.

Die Diskussion um AI im SOC schwankt 2026 zwischen zwei Extremen: Auf der einen Seite das Versprechen nahezu autonomer Security Operations, auf der anderen Seite die pauschale Skepsis gegenüber jeder Form von AI-Unterstützung. Die Realität liegt - wie so oft - dazwischen.

AI verändert Security Operations, aber nicht im Sinne eines Ersatzes menschlicher Expertise. Sie verändert die Art, wie Informationen verarbeitet, priorisiert und kommuniziert werden.

Der operative Mehrwert von AI im SOC zeigt sich vor allem in drei Bereichen: der Strukturierung großer Datenmengen, der Kontextualisierung von Alerts und der Beschleunigung dokumentationsintensiver Prozesse. Generative Modelle können technische Logdaten in verständliche Zusammenfassungen überführen, Hypothesen strukturieren und Übergaben zwischen Rollen erleichtern. Das reduziert kognitive Last, insbesondere im Triage-Prozess.

Doch AI ist kein autonomer Analyst. Sie entscheidet nicht über Containment-Maßnahmen, sie trägt keine Haftung, und sie ersetzt keine Hypothesenbildung bei komplexen Vorfällen.

Die entscheidende Differenzierung lautet daher: AI ist ein Beschleuniger von Verarbeitung, nicht von Verantwortung.

Gerade im Kontext von Effizienz muss diese Unterscheidung sauber getroffen werden. Automatisierte Standardreaktionen, wie etwa IOC-basierte Blockierungen, sind seit Jahren etabliert. AI ergänzt diese Mechanismen, indem sie Kontext schneller bereitstellt oder Muster erkennt, die regelbasiert schwer abzubilden sind. Doch sie ersetzt nicht die strukturellen Voraussetzungen effizienter Security Operations: saubere Detection-Logik, klare Playbooks und definierte Eskalationspfade.

Hinzu kommt eine neue Form von Komplexität. Generative Systeme formulieren überzeugend. Sie liefern plausible Begründungen, auch wenn die zugrunde liegende Kausalität unsicher ist. Dieses Phänomen, oft als „charming AI“ beschrieben, erzeugt ein epistemisches Risiko: Sprachliche Qualität wird mit analytischer Qualität verwechselt. Unter Zeitdruck kann das zu Fehlentscheidungen führen.

AI im SOC 2026 erfordert daher zusätzliche Governance. Wer AI einsetzt, muss definieren:

- Welche Entscheidungen dürfen automatisiert erfolgen?
- Welche Outputs sind prüfungspflichtig?
- Wie wird Modellverhalten überwacht?
- Wer trägt letztlich die operative Verantwortung?

Die Vorstellung eines vollständig autonomen SOC bleibt auch 2026 unrealistisch. Was realistisch ist, ist ein hybrides Modell: Automatisierte, regelbasierte Prozesse für standardisierbare Fälle, AI-gestützte Entscheidungsunterstützung bei komplexeren Szenarien und klare menschliche Letztverantwortung.

AI ist damit kein Ersatz für Struktur, sondern ein Verstärker bestehender Reife.

MDR & XDR: Orientierung im intransparenten Markt

Parallel zur technologischen Debatte verändert sich der Markt für Security Operations massiv. Managed Detection & Response (MDR), Managed SOC, XDR-as-a-Service. Die Begriffe sind zahlreich, ihre Definitionen jedoch selten konsistent.

Für viele Unternehmen entsteht 2026 ein Orientierungsproblem: Zwei Angebote tragen denselben Namen, basieren jedoch auf völlig unterschiedlichen Architekturen und Kompetenzmodellen.

Ein SOC-Angebot kann beispielsweise auf einem zentralen SIEM mit eigenem Detection Engineering basieren. Ein anderes nutzt primär EDR-Telemetrie mit eingeschränkter Log-Tiefe. Wieder ein anderes kombiniert SOAR-Orchestrierung mit punktueller Analystenunterstützung. Der Begriff allein sagt wenig über tatsächliche Leistungsfähigkeit aus.

Die Architekturfrage ist dabei nicht trivial. Ein SOC, das nur Endpoint-Daten auswertet, besitzt eine andere Sichtbarkeit als eines mit umfassender Cloud-, Netzwerk- und Identity-Telemetrie. Fehlt diese Transparenz in der Angebotsbeschreibung, entsteht eine Illusion von Vollständigkeit.

Hinzu kommt ein zweiter, oft unterschätzter Aspekt: Expertise.

Nicht jedes „24x7 SOC“ verfügt über klar getrennte Rollen wie Detection Engineer, Incident Responder oder Platform Engineer. In manchen Modellen übernehmen wenige Analysten mehrere Aufgaben parallel. Das kann bei kleinen Umgebungen funktionieren, skaliert jedoch nur begrenzt.

Für Unternehmen bedeutet das: Der Leistungsumfang eines SOC oder MDR-Anbieters hängt nicht nur von der Technologie ab, sondern vom zugrunde liegenden Rollenmodell.

- Gibt es dediziertes Detection Engineering?
- Existiert ein strukturiertes Incident-Response-Team?
- Wer verantwortet Plattformstabilität?
- Wer entwickelt Playbooks weiter?

Fehlt diese Spezialisierung, entsteht ein strukturelles Effizienzlimit.

Ein weiteres Problem liegt in der Intransparenz von Verantwortlichkeiten. „Monitoring 24x7“ bedeutet nicht automatisch „Incident Response 24x7“. Manche Modelle erkennen Vorfälle rund um die Uhr, überlassen jedoch Containment-Entscheidungen vollständig dem Kunden. Andere greifen aktiv ein, allerdings nur innerhalb klar definierter Standardfälle.

Für Entscheider ist daher weniger die Bezeichnung entscheidend als die Struktur dahinter. Drei Fragen sind zentral:

1. Welche Telemetrie wird tatsächlich verarbeitet?
2. Welche Rollen sind real besetzt?
3. Wo endet die Verantwortung des Anbieters und wo beginnt die des Kunden?

MDR ist keine falsche Lösung. In vielen Fällen ist es eine sinnvolle Antwort auf Fachkräftemangel und 24/7-Anforderungen. Problematisch wird es erst, wenn der Begriff operative Tiefe suggeriert, die strukturell nicht vorhanden ist.

Security Operations 2026 sind kein reines Make-or-Buy-Thema. Sie sind eine Frage von Transparenz, Rollenreife und klarer Verantwortungszuweisung.

Fazit: SOC 2026 ist ein Betriebsmodell

Security Operations im Jahr 2026 sind weder primär eine AI-Frage noch eine reine Outsourcing-Entscheidung. Sie sind Ausdruck organisatorischer Reife. Effizienz entsteht dort, wo Detection präzise, Prozesse klar definiert und Rollen eindeutig zugeordnet sind. Automatisierung - einschließlich AI - kann diese Struktur deutlich beschleunigen, insbesondere bei standardisierbaren Fällen. Sie ersetzt jedoch weder Verantwortung noch Expertise.

Gleichzeitig erfordert der wachsende Security-Service Markt eine differenzierte Betrachtung. Gleichlautende Begriffe stehen häufig für unterschiedliche Architekturen, Telemetrieabdeckung und Kompetenzmodelle. Entscheidend ist daher nicht die Bezeichnung eines Angebots, sondern die Transparenz über Rollen, Zuständigkeiten und Leistungsumfang.

Messbare Kennzahlen wie MTTD, MTTA und MTTR liefern dabei keine bloßen Reportingwerte, sondern Hinweise auf strukturelle Stärken und Schwächen. Sie machen Effizienz nachvollziehbar und steuerbar.

Security Operations sind damit kein Tool-Stack, sondern ein Betriebsmodell. Technologie kann dieses Modell leistungsfähiger machen. Ob es wirksam ist, entscheidet jedoch die Organisation, die es betreibt.

CISO-Takeaways für 2026

1. Effizienz im SOC ist ein Strukturthema, kein AI-Projekt.
2. MTTD, MTTA und MTTR sind Steuerungskennzahlen, keine Reporting-Zahlen.
3. Automatisierung reduziert Wartezeiten, nicht Verantwortung.
4. Rollen- und Prozessklarheit bestimmen die Wirksamkeit eines SOC.
5. MDR ist eine Architektur- und Governance-Entscheidung, kein Produktkauf.

Schlusswort:

2026 markiert keinen technologischen Wendepunkt, sondern einen Reifegradtest. Organisationen, die Effizienz strukturell verstehen, schaffen Stabilität trotz wachsender Komplexität.

Die Frage lautet nicht, ob AI eingesetzt wird oder ob ein MDR-Modell gewählt wird. Die Frage lautet, ob Verantwortlichkeiten eindeutig definiert, Prozesse messbar gesteuert und Entscheidungsbefugnisse klar geregelt sind.

Security Operations bleiben damit eine Führungsaufgabe. Technologie kann unterstützen. Struktur entscheidet.

Weitere Informationen zum Thema:

Podcast-Folge:

2025 im Rückblick.
2026 im Ausblick.
KI, NIS2 und die wichtigsten Cybersecurity-Trends

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
Web: www.suresecure.de