sure[secure]
your security operations center

# secure mag


## REALE USE-CASES UND MEHRWERTE VON AGENTIC AI SOCs

Was heute wirklich möglich ist und wie der europäische Markt den nächsten Schritt geht.

DAS SOC UNTER DRUCK

## WAS SICH IM BEDROHUNGS-UMFELD VERÄNDERT HAT

Angreifer arbeiten mit KI. Sie automatisieren Phishing-Kampagnen, komprimieren Breakout-Zeiten auf unter vier Minuten und skalieren Angriffsvektoren, die früher Wochen Vorbereitung kosteten. Was tun die Verteidiger? Zu oft: dasselbe wie immer. Zu langsam, zu manuell, zu reaktiv.

Security Operations Center leisten heute bemerkenswerte Arbeit unter Bedingungen, die sich in den letzten Jahren fundamental verändert haben. Die Teams sind gut, die Werkzeuge sind ausgereift, die Prozesse sind etabliert. Und trotzdem wächst eine strukturelle Diskrepanz zwischen dem, was ein SOC leisten kann, und dem, was die Bedrohungslandschaft inzwischen von ihm fordert.

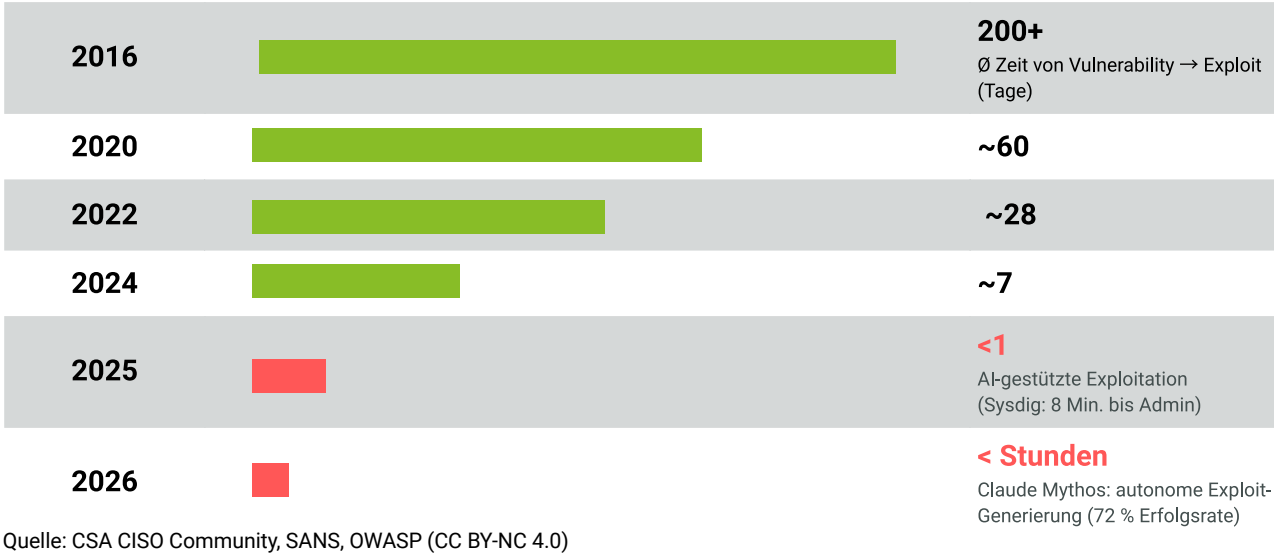
Die Zahlen illustrieren die Dimension dieser Veränderung: SOC-Teams erhalten heute durchschnittlich über 4.000 Alerts pro Tag, die große Mehrheit davon False Positives oder Low-Priority-Notifikationen. Laut dem SACR 2025 AI SOC Market Landscape Report bleiben 40 % aller Security-Alerts uninvestigiert. Nicht aus mangelndem Einsatz, sondern weil die Kapazität schlicht nicht ausreicht, um mit dem Volumen Schritt zu halten.

Noch deutlicher zeigt sich das Veränderungstempo auf der Angriffsseite. Und diese Beschleunigung ist kein plötzlicher Bruch, sie ist das Resultat einer mehrjährigen, gut dokumentierten Entwicklung.

| 4.000+ | 40 % | 4 Min. | 703 % |
|---|---|---|---|
| Alerts täglich im Ø SOC | der Alerts gehen uninvestigiert | Breakout-Zeit in schnellsten Fällen 2025 | Anstieg KI-gestützter Phishing-Angriffe |

FROM VULNERABILITY TO EXPLOIT:

## DER KOLLABIERTE ZEITKORRIDOR




Quelle: CSA CISO Community, SANS, OWASP (CC BY-NC 4.0)

Diese Entwicklung ist empirisch gut belegt. Sergej Epp (CISO, Sysdig) dokumentierte 2026 einen KI-basierten Angriff, der in acht Minuten Admin-Level-Zugang erlangte. Anthropics Claude Mythos entdeckte in einem kontrollierten Umfeld tausende Zero-Days über alle großen Betriebssysteme und Browser hinweg, mit einer Exploit-Erfolgsrate von 72 %; autonom, ohne menschliche Steuerung. Die Cloud Security Alliance, SANS, OWASP und Ex-NSA-Direktor Rob Joyce kommen in ihrem gemeinsamen Briefing vom April 2026 zu einer klaren Einschätzung: Die Asymmetrie zwischen Angriffs- und Verteidigungsgeschwindigkeit ist struktureller Natur.

ReliaQuest's Annual Threat Report 2026 belegt Lateral-Movement-Vorgänge in unter vier Minuten. Eine Beschleunigung um 85 % gegenüber dem Vorjahr. Das setzt SOC-Teams, die auf manuelle Triage angewiesen sind, unter erheblichen Zeitdruck und zeigt, wo Automatisierung den größten Hebel bietet.

**ANMERKUNG:** Der Zeitkollaps ist ein Leading Indicator für Angreifer-Kapazität, kein direktes Maß für Schadenshöhe. Die folgenreichsten Incidents der letzten Jahre erfolgten oft per Credential-Missbrauch oder Supply-Chain-Kompromittierung — nicht per Zero-Day.

> „If defense depends on human intervention to begin, defense will always feel asymmetrical."
>
> — Microsoft Security Blog, April 2026

Dazu kommt die menschliche Komponente: Laut SANS SOC Survey fühlen sich 80 % der Analysten chronisch im Rückstand. Osterman Research stellt fest: 90 % der SOCs kämpfen mit Alert-Backlogs und hohen False-Positive-Raten. Das sind keine Versagenssignale, das sind Zeichen eines Systems, das an seine Kapazitätsgrenzen stößt. Und genau hier setzt Agentic AI an.

## WAS IST AGENTIC AI,
## UND WAS IST ES NICHT?

Bevor wir in die Praxis gehen, brauchen wir eine saubere Begriffsklarheit. Denn „Agentic AI“ ist 2025 zum meistzitierten Begriff der Cybersecurity-Industrie geworden und damit auch zum meist verwässerten. Nahezu jeder Vendor wirbt mit „AI Agents“. Was darunter zu verstehen ist, variiert erheblich.

### DER UNTERSCHIED, DER ZÄHLT

Traditionelle Automatisierung (SOAR) funktioniert nach dem Muster: „Wenn Alert-Typ X, führe Playbook Y aus.“ Das ist deterministische Logik; zuverlässig, nachvollziehbar, auditierbar. Sehr gut für wiederkehrende, klar definierte Szenarien. Aber begrenzt in der Flexibilität, wenn ein Vorfall vom bekannten Muster abweicht.

Agentic AI denkt anders. Ein echter AI-Agent verfolgt Ziele statt Instruktionen. Er bekommt den Auftrag: „Untersuche diesen Alert und bestimme, ob er eine echte Bedrohung darstellt.“ Dann wählt er autonom, welche Tools er abfragt, wie er die Ergebnisse korreliert und welche Handlung er empfiehlt oder ausführt, auch bei vollkommen neuen Angriffsmustern.

Ein modernes Agentic SOC basiert typischerweise auf einem Multi-Agent-System (MAS): spezialisierte Agenten für Triage, Threat Intelligence, Incident Response, Cloud Security und Compliance arbeiten koordiniert zusammen. Kein Monolith, sondern ein Team von Maschinen, mit einem Orchestrierungsagenten, der den Gesamtprozess steuert.

Wichtig: Echte Agentic-AI-Systeme arbeiten 2025 ausnahmslos nach dem „Human-in-the-Loop“- oder „Human-on-the-Loop“-Prinzip. Der Mensch entscheidet über irreversible, rechtlich relevante oder strategisch kritische Maßnahmen. Die KI übernimmt das Volumen - der Analyst übernimmt das Urteil.

Was Agentic AI kann

- Ziele verfolgen statt Regeln folgen
- Multi-Step-Aufgaben autonom ausführen
- Mit unvollständigen Informationen umgehen
- Aus Ergebnissen lernen und Verhalten anpassen
- Mehrere spezialisierte Sub-Agenten koordinieren (Multi-Agent-System)

„Smaller, specialized language models often outperform their massive general-purpose counterparts in security operations. SOC environments increasingly favor models in the 100 million to 7 billion parameter range.“

— EY Insights, April 2026

REALE USE-CASES:

# WAS HEUTE SCHON LÄUFT

Kein Proof-of-Concept, kein Lab-Experiment. Die folgenden Use-Cases sind produktiv im Einsatz: in Fortune-500-Unternehmen, bei MSSPs und in mittelgroßen Security-Teams. Jeder Use-Case ist entlang von drei Nutzendimensionen eingeordnet:

1. **Effizienz**
   weniger Aufwand für gleiches Ergebnis
2. **Wirksamkeit**
   besseres Ergebnis mit gleichem Aufwand
3. **Qualität**
   Zuverlässigkeit, Konsistenz, Nachvollziehbarkeit der Arbeit

USE-CASE 01

## AUTONOMES ALERT-TRIAGE & INVESTIGATION

Ein AI-Agent empfängt eingehende Alerts, korreliert sie eigenständig mit Threat-Intelligence-Feeds, fragt Endpoint-Telemetrie und Identity-Logs ab, bewertet den Schweregrad und liefert innerhalb von Sekunden einen vollständigen Investigation-Report. Der Analyst erhält keine rohe Alert-Queue mehr, sondern eine Liste voruntersuchter Fälle - angereichert, priorisiert, mit Kontext.

**Effizienzgewinn:** Laut SACR 2025 dauert eine durchschnittliche Alert-Investigation 70 Minuten. Agentic-AI-Deployments reduzieren das auf unter 10 Minuten, bei gleichzeitig höherer Konsistenz, weil der Agent denselben Prozess für Alert Nr. 1 und Alert Nr. 4.000 identisch ausführt. Menschliche Ermüdungseffekte, die spät in der Schicht zu Fehlern führen, entfallen.

**Wirksamkeitsdimension:** Der größte Hebel liegt weniger in der Geschwindigkeit als in der Coverage. Alerts, die heute aus Kapazitätsgründen nicht untersucht werden, werden es mit Agentic AI. Das verändert die Schutztiefe fundamental.

**Qualitätsgewinn:** Jede Investigation läuft nach demselben nachvollziehbaren Prozess ab und wird vollständig protokolliert — inklusive der Threat-Intelligence-Quellen, die zur Bewertung geführt haben. Das schafft eine Konsistenz und Auditierbarkeit, die manuelle Triage in der Praxis selten erreicht, weil sie von Erfahrung, Tagesform und Zeitdruck des jeweiligen Analysten abhängt.


USE-CASE 02

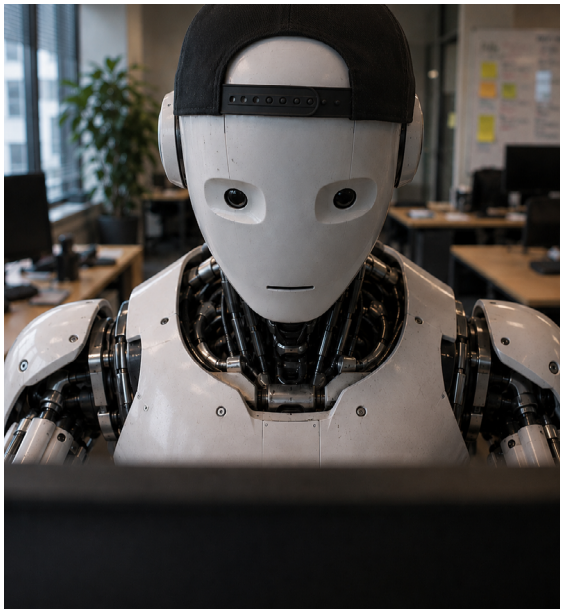
## AUTOMATISIERTE EDR-RESPONSE

Wenn SentinelOne oder CrowdStrike einen Endpoint-Vorfall melden, startet der AI-Agent sofort eine koordinierte Reaktion; Asset-Details aus dem CMDB abrufen, korrelierte User-Aktivität prüfen, betroffenen Host quarantänisieren, kompromittierte Credentials flaggen, Report autogenerieren. Der gesamte Prozess läuft in Sekunden, ohne Wartezeit auf den nächsten verfügbaren Analysten.

**Wirksamkeitsdimension:** Der entscheidende Unterschied liegt im Zeitfenster. ReliaQuest dokumentierte Lateral-Movement in unter vier Minuten, schneller als jede manuelle Triage-Kette. Ein AI-Agent, der Containment-Maßnahmen innerhalb von Sekunden initiiert, verkürzt den Blast Radius eines Angriffs erheblich.

**Qualitätsgewinn:** Der Prozess ist vollständig auditierbar, jeder Schritt protokolliert, jede Entscheidung nachvollziehbar. Wertvoll für Compliance-Anforderungen unter NIS2.

**Praxisbeleg:** Torq-Kunden berichten von MTTR-Reduktionen um 60–90 Prozent nach Einführung automatisierter EDR-Response-Workflows. Kenvue erzielte 60 % MTTR-Verbesserung in zwei Monaten.



USE-CASE 03

## PHISHING-RESPONSE-AUTOMATISIERUNG

Phishing ist und bleibt der meistgenutzte Angriffsvektor. Ein AI-Agent überwacht das Security-Postfach kontinuierlich, extrahiert URLs, Anhänge und Header-IPs aus jeder eingehenden Meldung und übergibt sie an VirusTotal und weitere Threat-Intel-Dienste. Basierend auf den Ergebnissen kategorisiert er automatisch als malicious, suspicious oder clean und startet bei Bedarf sofort Remediation-Workflows, ohne dass ein Analyst eingreifen muss.

**Effizienzgewinn:** Was früher Stunden manueller Arbeit bedeutete — Meldung entgegennehmen, URL extrahieren, prüfen, klassifizieren, eskalieren oder schließen — läuft nun in Sekunden. Valvoline berichtete nach Torq-Einführung von sieben Stunden eingespartem Analysten-Workload pro Tag, ein Großteil davon durch Phishing-Automatisierung.

**Qualitätsgewinn:** KI-gestützte Phishing-Klassifikation ist konsistenter als manuelle Einschätzungen, die von Tageszeit, Erfahrungsgrad und Auslastung abhängen.


USE-CASE 04

## IDENTITY & ACCESS MANAGEMENT (IAM) AUTOMATION

Identity ist heute das primäre Angriffsziel. Der Großteil aller Breaches beginnt mit kompromittierten Credentials. AI-Agenten überwachen kontinuierlich auf Anomalien: Impossible-Travel-Events (Login aus Frankfurt, dann drei Minuten später aus Singapur), ungewohnte Login-Zeiten, wiederholte MFA-Ablehnungen als Indiz für Fatigue-Angriffe. Bei Erkennung reagieren sie automatisch: Account temporär sperren, Credential-Reset initiieren, User über sichere Kanäle zur Verifikation auffordern.

**Wirksamkeitsdimension:** Die entscheidende Stärke ist die 24/7-Kontinuität ohne Qualitätsverlust. Impossible-Travel um 3 Uhr nachts wird genauso zuverlässig erkannt wie um 14 Uhr mittags.

**Qualitätsgewinn:** Automatische Dokumentation jedes IAM-Ereignisses und jeder Gegenmaßnahme schafft einen lückenlosen Audit-Trail. Eine direkte Anforderung unter NIS2 und DORA. Ein manueller Prozess erzeugt diese Aufzeichnung selten in der erforderlichen Granularität.

USE-CASE 05

## CLOUD-SECURITY-MONITORING & MISCONFIGURATION RESPONSE

Cloud-Umgebungen produzieren ein Telemetrie-Volumen, das manuelle Auswertung scheitern lässt. AWS CloudTrail allein erzeugt in mittelgroßen Umgebungen hunderte Gigabyte pro Tag. AI-Agenten überwachen kontinuierlich auf Misconfigurations (offene S3-Buckets, zu weit gefächerte IAM-Policies, öffentlich exponierte Services), unautorisierte Datenzugriffe und anomale Netzwerkmuster, über alle Cloud-Provider gleichzeitig.

**Wirksamkeitsdimension:** Cloud-Security-Vorfälle stiegen 2024 um 89 %. Die Dynamik von Cloud-Infrastruktur — neue Services, veränderliche Konfigurationen, kurzlebige Instanzen — macht statische Regelwerke schnell obsolet. AI-Agenten passen ihre Basisline kontinuierlich an die tatsächliche Umgebung an, statt gegen ein starres Regelwerk zu prüfen. Ein weiterer Aspekt: Misconfiguration-Detection ist in vielen Unternehmen heute reaktiv (Pentest oder Incident führt zur Erkenntnis). Agentic AI macht sie kontinuierlich und proaktiv.

**Qualitätsgewinn:** Da der Agent dieselben Prüfkriterien konsequent über jede Cloud-Ressource und jeden Account hinweg anwendet, entstehen weniger blinde Flecken durch Stichproben oder unterschiedliche Prüftiefe einzelner Teammitglieder. Jede erkannte Abweichung wird mit Kontext dokumentiert — eine wertvolle Grundlage für Audits und für die kontinuierliche Verbesserung der eigenen Cloud-Architektur.

USE-CASE 06

## AUTONOME ANGRIFFSUNTERBRECHUNG (ATTACK DISRUPTION)

Dieser Use-Case ist der fortgeschrittenste und derjenige, der das größte Umdenken erfordert. Bei einem laufenden Angriff — etwa einem Credential-Theft-Versuch — sperrt das System automatisch den betroffenen Account und isoliert das kompromittierte Gerät, noch bevor Lateral Movement beginnen kann.

Gleichzeitig startet ein AI-Agent eine vollständige Untersuchung über Identity-, Endpoint-, E-Mail- und Cloud-Signale und konsolidiert alles in einer einzigen, priorisierten Ansicht für den Analysten.

**Wirksamkeitsdimension:** Das Entscheidende ist das Zeitfenster. In der Phase zwischen erstem Zugang und Lateral Movement (heute oft unter vier Minuten) kann ein autonom agierendes System den Angriffsablauf unterbrechen, bevor Schaden entsteht. Kein Analyst kann in dieser Geschwindigkeit manuell reagieren.

**Qualitätsgewinn:** Die Kombination aus schnellem Containment und vollständiger Dokumentation — was wurde wann gesperrt, welche Signale lagen vor, welche Maßnahmen wurden ergriffen — ermöglicht außerdem eine präzisere Post-Incident-Analyse und stärkt die Lernfähigkeit des Systems.


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...

WER BAUT DAS?

# ANBIETER UND PLATTFORMEN IM ÜBERBLICK

Der Markt ist in Bewegung: Omdia trackt aktuell mehr als 50 Agentic-SOC-Startups, gleichzeitig integrieren etablierte Plattformen wie Microsoft und Google AI-Agenten tief in ihre bestehenden Security-Stacks. Die folgende Übersicht strukturiert die relevantesten Ansätze; von Pure-Play-Startups bis zu Hyperscaler-Plattformen und Workflow-Enablement-Tools.

| Anbieter | Ansatz | Stärken | Zielgruppe | Preismodell | Referenz-Kunden |
|---|---|---|---|---|---|
| Torq HyperSOC | Pure-Play Agentic, Multi-Agent (MAS) | Kein Code nötig, elastische Skalierung, 10x schneller als SOAR | Enterprise, Fortune 500, MSSPs | Pro-Use-Case / Platform-Fee; $140M Series-D 2026 | Siemens, Virgin Atlantic, Marriott, PepsiCo |
| Microsoft Sentinel + Copilot | Plattform-integriert, nativer Stack | Nahtlose M365/Azure-Integration, breite Anbieterbasis | Microsoft-Shops, Enterprise | Per-User/Node, als Azure-Add-on | Tausende Enterprise-Kunden weltweit |
| Google SecOps (Chronicle) | Agentic über MCP, Cloud-native | Multi-Vendor via MCP, starke Cloud-Telemetrie | Google-Cloud-Kunden, Enterprise | Consumption-based, Google Cloud Pricing | Große US-Enterprise-Kunden |
| Dropzone AI | Autonomer AI-Analyst, no Playbook | 100 % Alert-Coverage, 90 % MTTC-Reduktion, kein Code | Mid-Market, MSSP | Per-Alert oder per Seat | Fortune-500-SOCs (anonym) |
| DXC + 7AI | Managed, vollautonomer MSSP-Layer | 24/7 managed, sofort einsatzbereit, globale Skalierung | Enterprise, Outsourcing | Managed Service, kundenspezifisch | DXC-Bestandskunden global |
| Tines | Workflow-Automation-Layer | No-Code, vendor-agnostisch, sehr flexibel | Alle Größen, tech-affine Teams | Seat-basiert, Community-Edition verfügbar | Elastic, Coinbase, Reddit, GitLab |

TORQ:

## HYPERSOC

Torq hat sich 2025/2026 als der am schnellsten wachsende Agentic-SOC-Anbieter im Enterprise-Segment etabliert. Die Plattform kombiniert ein Multi-Agent-System — mit „Socrates“ als zentralem Orchestrierungsagenten — mit einer Hyperautomation-Engine, die komplexe Security-Workflows no-code in Minuten statt Monaten aufbaut. Besonderes Merkmal: Torq funktioniert als Orchestrierungsschicht über dem bestehenden Tool-Stack. Ersetzt nichts, verbindet aber alles. Im Januar 2026 sicherte Torq sich eine Series-D-Finanzierung von 140 Millionen Dollar bei einer Bewertung von 1,2 Milliarden Dollar; getrieben durch die starke Nachfrage aus Fortune-500-Umgebungen, in denen CrowdStrike, SentinelOne und Microsoft bereits im Einsatz sind.

Aus Evaluierungsperspektive relevant: Torq zielt primär auf Unternehmen mit einem dedizierten Security-Team, das bereits Erfahrung mit SOAR-Tools hat. Der Einstieg ist niedrigschwellig (kein Code, keine Playbooks erforderlich), skaliert aber auch für hochkomplexe Enterprise-Workflows. Proof of Concept typischerweise in 30–60 Tagen möglich.

„Torq has transformed efficiency for all five of my security teams and enabled them to focus on much more high-value strategic work.“

— Enterprise CISO, Torq Customer

## MICROSOFT SENTINEL + SECURITY COPILOT

Microsoft verfolgt eine Plattform-Strategie: Agentic-AI-Fähigkeiten sind nativ in Sentinel, Defender und den gesamten Microsoft-Security-Stack integriert. Der strukturelle Vorteil liegt in der Datenbasis: Identity-Signale aus Entra, Endpoint-Daten aus Defender, E-Mail-Kontext aus Exchange und Cloud-Telemetrie aus Azure. Alles in einer einheitlichen, nativ korrelierten Schicht. Security Copilot bringt auf dieser Basis LLM-gestützte Investigation, automatische Playbook-Generierung und natürlichsprachliche Abfragen („Zeige mir alle Logins aus Russland der letzten 24 Stunden“).

Für Unternehmen, die bereits tief im Microsoft-Stack sind, ist dieser Ansatz der Weg des geringsten Widerstands. Die Einschränkung: Die Stärke hängt stark davon ab, wie viel des Security-Stacks bereits Microsoft ist. Gemischte Umgebungen profitieren weniger. Dokumentierte Ergebnisgrößenordnung: 30 % MTTR-Reduktion.

GOOGLE CLOUD SECURITY:

## AGENTIC SOC

Google setzt mit seiner Chronicle-SIEM-Plattform auf einen anderen Ansatz: AI-Agenten kommunizieren via Model Context Protocol (MCP) mit dem gesamten Security-Stack, nicht nur Google-Produkten. Das schafft Multi-Vendor-Fähigkeiten, die für heterogene Umgebungen relevant sind. Der Alert-Triage-Agent investigiert vollständig autonom — inklusive Dekodierung verschleierter Scripts und Cross-Source-Korrelation — und liefert ein Untersuchungsergebnis mit Erklärung, das dem Analysten die Entscheidungsfindung abnimmt, nicht nur die Datensuche. Dokumentierte Größenordnung: 50 % schnellere MTTR.

## DROPZONE AI

Dropzone AI repräsentiert den radikalsten Ansatz im Markt: Ein vollständig autonomer AI-SOC-Analyst, der ohne Playbooks, Konfigurationsaufwand oder manuelles Prompting arbeitet. Der Agent untersucht jeden Alert mit dem gleichen Prozess, den ein erfahrener Tier-1-Analyst anwenden würde. Nur schneller, konsistenter und ohne Tageszeit oder Auslastung als Variable. Gartner ernannte Dropzone zum Cool Vendor for the Modern SOC. Aus einer anderen Quelle: 150 CISOs wählten Dropzone in den Rising in Cyber 2025-Report. Dokumentierte Ergebnisse in Produktion: 90 % Reduktion der Mean Time to Conclusion (von 20–40 Minuten auf 3–10 Minuten), 100 % Alert-Coverage bei deployten Kunden.

## DXC TECHNOLOGY + 7AI

DXC ist ein anderer Ansatz: kein Tool zum Selbstbetreiben, sondern ein Managed Service, der Agentic AI komplett übernimmt. DXC verarbeitet täglich 4,5 Millionen Bedrohungen über 3.200 Security-Experten in 12 SOCs weltweit und integriert seit 2025 7AIs autonome Plattform als Kerntechnologie für vollständig autonome Agenten vom Alert-Eingang bis zur Remediation. Für Organisationen, die Security komplett auslagern möchten, ist dieses Modell der direkteste Weg zu Agentic-AI-Fähigkeiten ohne interne Aufbauzeit.

## TINES

Tines ist weniger ein Agentic SOC als ein Enablement-Layer, der Agentic-AI-Workflows überhaupt erst möglich macht. Die no-code Plattform verbindet beliebige Tools, lässt Security-Analysten ohne Programmierkenntnis komplexe Automatisierungen aufbauen und integriert LLM-Capabilities für kontextsensitive Entscheidungen. Elastic setzt Tines intern ein und schätzt, dass die Plattform die Arbeit von 95 Vollzeit-Analysten übernimmt, aufgebaut von einem relativ kleinen Team. Besonderer Vorteil: vendor-agnostisch, Community-Edition verfügbar, niedrige Einstiegshürde.

## MESSBARE ERGEBNISSE
## AUS DER PRAXIS

Kein Vendor-Versprechen ohne Beweis. Die folgenden Zahlen stammen aus dokumentierten, produktiven Deployments:

| Unternehmen | Maßnahme | Ergebnis |
|---|---|---|
| Kenvue | Outsourced SOC -> Torq in-house | 60 % MTTR-Reduktion in 2 Monaten, 89 % Auto-Remediation |
| Valvoline | Torq AI SOC Platform | 7 Stunden Analyst-Workload/Tag eingespart |
| Virgin Atlantic | Torq Hyperautomation | 40+ Stunden manueller Arbeit pro Woche eliminiert |
| Carvana | Agentic AI Tier-1-Handling | 100 % der Tier-1-Alerts autonom, kein Headcount-Anstieg |
| Transurban | 2 spezialisierte AI-Agenten | Von 8 % auf signifikant höhere Alert-Coverage |
| Dropzone AI Kunden | Autonom. Investigation | 90 % Reduktion MTTC (20–40 Min. -> 3–10 Min.) |

Was diese Zahlen vereint: Sie kommen alle aus Produktivumgebungen, nicht aus kontrollierten Tests. Und sie zeigen ein konsistentes Muster: Effizienzgewinne von 60 bis 95 % in Triage, Investigation und Remediation, kombiniert mit dem entscheidenden Effekt: Analysten werden von Tier-1-Fleissarbeit befreit.

**ACHTUNG: EINORDNUNG**

Die meisten publizierten Zahlen stammen von den Anbietern selbst oder aus gemeinsam erstellten Case Studies. Unabhängige Drittvalidierungen sind noch rar. IDC und Gartner liefern zunehmend externe Einschätzungen. Die Größenordnung der Ergebnisse wird aber auch von neutralen Quellen bestätigt.

WAS KOSTET DAS?

# INVESTITION UND ROI IN DER EINORDNUNG

Einer der häufigsten Gründe, warum Agentic-AI-Projekte im Genehmigungsprozess stecken bleiben: fehlende Kostenklarheit. Der Markt ist intransparent, und diese Intransparenz hat Methode. Laut UnderDefense's AI SOC Pricing Guide 2026 unterschätzen die meisten Käufer ihre tatsächlichen Gesamtkosten um 25–40 %, weil versteckte Gebühren, Overage-Klauseln und Add-on-SKUs erst nach Vertragsunterzeichnung sichtbar werden.

Die grundsätzliche Make-or-Buy-Entscheidung lässt sich dabei mit Marktdaten gut unterlegen: Ein intern aufgebautes SOC kostet laut Ponemon Institute im Durchschnitt 2,84 Millionen Dollar jährlich; bei 5–8 FTEs, eigener SIEM-Infrastruktur und einer Aufbauzeit von 6–18 Monaten. Klassische MSSPs, die primär Alert-Monitoring ohne echte Response bieten, liegen bei 100.000 bis 500.000 Dollar jährlich, mit dem Haken, dass Investigation und Reaktion nach wie vor beim eigenen Team verbleiben.

Für die ROI-Argumentation gegenüber Entscheidern empfiehlt sich eine dreigliedrige Rechnung: Kostenersparnis durch höhere Automatisierung (FTE-Äquivalent), Schadenvermeidung durch schnellere Reaktionszeiten (probability-weighted: 15 % Jahreswahrscheinlichkeit eines Breaches × durchschnittliche Schadenskosten) und Versicherungsprämien-Reduktion durch nachweisbare 24/7-Coverage. Nach diesem Modell (berechnet für 1.000 Endpoints) lässt sich ein ROI von über 150 % mit einem Payback-Zeitraum von unter einem Jahr darstellen.

Wichtig: Die Einzel-Annahmen (Schadenshöhe, FTE-Kosten, Prämienentwicklung) sollten im eigenen Kontext validiert werden, die Rechenmethodik ist aber mit publizierten Industriedaten belastbar.

| Modell | Typische Jahreskosten (Mid-Market) | Aufbauzeit | Response-Fähigkeit |
|---|---|---|---|
| In-house SOC (Build) | 1,2–2 Mio. € | 6–18 Monate | Vollständig (wenn besetzt) |
| Klassischer MSSP | 100–500 T€ | 1–3 Monate | Alert-Eskalation, Response beim Kunden |
| Agentic AI SOC (Managed) | 100–200 T€ | 30 Tage | Detection + autonome Response inkl. |
| Agentic AI SOC (Plattform) | variabel nach Plattform | 30–60 Tage PoC | Je nach Deployment-Tiefe |

**Worauf beim Pricing besonders achten?**

- Preismodell: Per-Endpoint ist planbar, Per-GB-Ingestion führt zu Budgetüberschreitungen, sobald Cloud-Workloads wachsen.
- Hidden Fees: Onboarding, Compliance-Reporting, IR-Retainer und Daten-Retention sind häufige Zusatzkosten, die im Erstangebot fehlen.
- Vertragsbedingungen: Automatische Preiserhöhungsklauseln (5–8 % p.a.) und nicht kündbare Multi-Year-Verträge sollten vor Unterzeichnung verhandelt werden.

# STAND, CHANCEN UND HEMMNISSE

Ehrliche Einschätzung: Europa ist nicht langsam, weil es zurückgeblieben ist. Es ist vorsichtig, weil es mehr zu verlieren hat; regulatorisch, kulturell und in Sachen Datensouveränität. Das ist kein Mangel, sondern eine andere Ausgangslage. Und diese Ausgangslage lässt sich gestalten.

## REGULIERUNG ALS RAHMEN UND ALS GESTALTUNGSAUFGABE

Europa hat 2025/2026 einen regulatorischen Umbruch erlebt: NIS2 (in Deutschland final verabschiedet November 2025), EU AI Act (vollständig anwendbar ab August 2026), Cyber Resilience Act, DORA und der Data Act greifen gleichzeitig. Für Unternehmen ist das zunächst eine erhebliche Aufgabe. Langfristig schafft es aber auch Klarheit: über Anforderungen, Verantwortlichkeiten und Standards, die in den USA in dieser Verbindlichkeit nicht existieren.

Für Agentic AI SOCs bedeutet das: Der EU AI Act stuft autonome Systeme mit sicherheitskritischen Entscheidungen möglicherweise als Hochrisiko-KI ein, mit entsprechenden Dokumentations- und Aufsichtspflichten. Wer das von Anfang an mitdenkt, baut robustere, vertrauenswürdigere Systeme. Wer es ignoriert, zahlt später.

„Datenschutz ist 2026 kein abstraktes Compliance-Thema mehr, sondern Teil der unternehmerischen Sorgfalt."

— Law-Blog.de, Januar 2026

## DSGVO: ANFORDERUNG UND QUALITÄTSMERKMAL

Agentic AI SOCs verarbeiten große Mengen sicherheitsrelevanter Daten, darunter User-Activity-Logs, Identity-Daten und E-Mail-Metadaten. Die DSGVO-Grundsätze der Datenminimierung, Zweckbindung und Erklärbarkeit (Art. 22 DSGVO) sind dabei keine zusätzliche Hürde, sondern ein sinnvoller Gestaltungsrahmen. Wer sie technisch implementiert — statt nur juristisch zu dokumentieren — baut Systeme, denen Nutzer und Aufsichtsbehörden gleichermaßen vertrauen.

Weitere Faktoren, die den Markt prägen

- Teamgröße und Ressourcen: 60 % europäischer Security-Teams haben weniger als 10 Mitglieder (IDC 2025). AI-Governance-Know-how muss erst aufgebaut werden. Das ist eine Investition, keine Schwäche.
- ROI-Nachweis: Der Business Case für KI-Investitionen ist in europäischen Mittelstands-Strukturen anspruchsvoller, braucht aber auch nur einmal überzeugend geführt werden, wie die dokumentierten Praxisergebnisse zeigen.
- Anbieterauswahl: Die führenden Plattformen kommen aus den USA. Datenresidenz in der EU, On-Premise-Optionen und vertragliche Steuerbarkeit sind berechtigte Anforderungen und werden zunehmend erfüllt.
- Zertifizierungs-Aufwand: NIS2-konforme Deployments erfordern Nachweise und Dokumentation. Der Aufwand ist real, aber auch ein Differenzierungsmerkmal gegenüber weniger sorgfältig aufgestellten Wettbewerbern.

Wann ist der Moment für europäische Unternehmen?

Omdia erwartet, dass Agentic-SOC-Fähigkeiten innerhalb von 1-2 Jahren zum Standard-Toolset von CISOs weltweit gehören werden. Für den deutschen Markt (Mittelstand und KRITIS-Unternehmen) ist 2026/2027 das realistische Adoptions-Fenster.

- Treiber: NIS2-Compliance-Druck, wachsender Fachkräftemangel und zunehmend EU-konforme Plattformangebote. Wer jetzt beginnt, Erfahrungen aufzubauen, hat in zwei Jahren einen echten Vorsprung.

KRITISCHE EINORDNUNG:

# WAS AGENTIC AI NICHT KANN

Ein seriöser Blick auf Agentic AI SOCs gehört dazu: Was sind die Grenzen heutiger Systeme, und wo liegt die Verantwortung des Menschen? Das sind keine Schwachstellen der Technologie. Es sind bewusste Designentscheidungen, über die IT-Entscheider informiert sein müssen.

1. **Menschliche Überwachung = Unverzichtbar**

   In allen produktiven Deployments 2025 gilt: Für Entscheidungen mit irreversiblen, rechtlichen oder strategischen Auswirkungen bleibt der Mensch in der Verantwortung. Das ist kein vorläufiger Kompromiss, sondern ein durchdachtes Designprinzip. Es schafft Vertrauen, erfüllt regulatorische Anforderungen und ist der Grund, warum diese Systeme in Enterprise-Umgebungen funktionieren.

2. **Modellverhalten und False Confidence**

   LLM-basierte Systeme können mit hoher Zuversicht falsch liegen. Das gilt für alle KI-Anwendungen, nicht nur für Security. Im SOC-Kontext bedeutet das: Audit-Logging, Governance Frameworks und regelmäßige Kalibrierung sind keine optionalen Extras, sondern Teil eines professionellen Deployments.

3. **Datenqualität als Grundvoraussetzung**

   AI-Agenten arbeiten mit dem, was gemessen wird. Wer mit fragmentierter Infrastruktur, heterogenen Log-Quellen oder lückenhafter CMDB startet, sollte zunächst in die Datenbasis investieren. Agentic AI verstärkt, was vorhanden ist. Es ersetzt keine Datenarchitektur.

## 4. Das Mythos-Problem: Angreifer holen auf

Die vielleicht unbequemste Wahrheit liefert ein Dokument, das im April 2026 von der Cloud Security Alliance gemeinsam mit SANS, OWASP, Heather Adkins (CISO, Google), Rob Joyce (ehem. Cybersecurity Director, NSA), Bruce Schneier und weiteren Top-CISOs veröffentlicht wurde: Anthropics Claude Mythos hat bewiesen, dass autonome KI-Systeme bereits heute tausende kritischer Schwachstellen in allen großen Betriebssystemen und Browsern entdecken und funktionierende Exploits generieren können, ohne menschliche Steuerung, mit einer Erfolgsrate von 72 %.

Was das für das Agentic AI SOC bedeutet: Die gleichen Fähigkeiten, die Defensivteams stärken, stehen auch Angreifern zur Verfügung, und oft früher. Durchschnittliche Kriminelle erhalten schrittweise Zugang zu Fähigkeiten, die früher Ressourcen auf Nationalstaatsniveau erforderten.

> „We cannot outwork machine-speed threats. Re-prioritize, automate, and prepare for burnout."
>
> — CSA CISO Community / SANS / OWASP: „The AI Vulnerability Storm", April 2026

Das CSA-Papier formuliert den dringendsten Handlungsauftrag für CISOs: nicht auf Perfektion warten, sondern jetzt mit AI-gestützter Verteidigung beginnen. Wer das nicht tut, überlässt die Geschwindigkeitsasymmetrie den Angreifern.

**Was bedeutet das konkret?**

AI-gestützte Vulnerability-Discovery läuft heute bereits in beide Richtungen. Unternehmen, die Agentic AI defensiv einsetzen, finden ihre eigenen Schwachstellen schneller als Angreifer. Unternehmen, die das nicht tun, warten darauf, dass jemand anderes sie findet.

## 5. Integration setzt Vorbereitung voraus

Die überzeugendsten Ergebnisse entstehen in Umgebungen mit sauberer Datenarchitektur, stabilen API-Integrationen und einem gepflegten Security-Stack. Das ist kein Ausschlussgrund, aber ein guter Hinweis, wo der Einstieg am sinnvollsten beginnt: mit einem klar abgegrenzten Use-Case, idealem Datenfluss und messbarem Ziel. Von dort skaliert man.

> „Organizations that approach agentic AI as a headcount replacement rather than a capability amplifier will design their deployments incorrectly, accepting risks that the technology was not designed to absorb."
>
> — Brandefense Research, April 2026

## FAZIT:

Agentic AI SOC ist kein Zukunftsthema. Es ist ein Gegenwartsthema für diejenigen, die verstanden haben, wie sich die Bedrohungslandschaft entwickelt hat, und für diejenigen, die ehrlich genug sind, zuzugeben, dass manuelle SOC-Prozesse strukturell nicht mehr mithalten.

Die heute führenden Unternehmen — Kenvue, Valvoline, Virgin Atlantic, Carvana, Siemens — haben nicht auf perfekte Bedingungen gewartet. Sie haben mit konkreten Use-Cases angefangen, Ergebnisse gemessen und Vertrauen aufgebaut. Das ist das Playbook.

Für den europäischen Markt gilt: Die regulatorische Komplexität ist real, aber sie ist kein Ausschlussgrund. Sie ist ein Gestaltungsrahmen. Wer NIS2, EU AI Act und DSGVO von Beginn an in seine Agentic-AI-Architektur einbaut, schafft nicht nur Compliance, sondern Wettbewerbsfähigkeit.

## CISO
## TAKEAWAYS

- Das traditionelle SOC ist strukturell überfordert. Alert-Volumen, Breakout-Zeiten und KI-gestützte Angriffe machen manuelle Prozesse zu einem systematischen Sicherheitsrisiko.
- Agentic AI ist kein SOAR-Upgrade. Es ist ein fundamental anderes Betriebsmodell, von Regelfolgen zu Zielverfolgung, von reaktiv zu antizipatorisch.
- Die Ergebnisse sind dokumentiert und reproduzierbar: 60-90 % MTTR-Reduktion, 89-100 % Auto-Remediation-Quoten und signifikante Analyst-Entlastung sind in Produktivumgebungen erreicht worden
- Human-in-the-Loop ist kein Kompromiss, sondern Design-Prinzip. Autonome KI übernimmt das Volumen, Menschen treffen die Urteile.
- Der europäische Markt braucht dringend Adoption, aber muss DSGVO, EU AI Act und NIS2 von Anfang an mitdenken. Das ist machbar, erfordert aber architektonische Vorarbeit.
- Die Frage ist nicht ob, sondern wann und wie. Claude Mythos hat gezeigt: KI-gestützte Angriffswerkzeuge sind Realität. Der Aufbau KI-gestützter Verteidigung ist deshalb keine optionale Modernisierung, sondern eine strategische Notwendigkeit.

## SCHLUSSWORT:

Agentic AI ist kein Zukunftsversprechen mehr. Die Technologie wird bereits produktiv eingesetzt und zeigt messbare Ergebnisse. Gleichzeitig steigen die Anforderungen an Geschwindigkeit, Skalierbarkeit und Verfügbarkeit in der Cyberabwehr weiter an. Für Unternehmen geht es deshalb nicht darum, ob sie sich mit Agentic AI beschäftigen sollten, sondern wie sie den Einstieg sinnvoll gestalten.

Wer heute beginnt, Erfahrungen aufzubauen, schafft die Voraussetzungen, um den Herausforderungen der nächsten Jahre mit größerer Resilienz und Handlungsfähigkeit zu begegnen.

## Weitere Informationen zum Thema:


Podcast-Folge:

Michael und Andreas sprechen über Agentic AI SOCs, autonome Security Operations und die Erkenntnisse der Google Cloud Next '26. Im Fokus steht die Frage, wie KI die Cyberabwehr verändert und warum moderne SOCs vor einem grundlegenden Wandel stehen.

Ausgewählte Quellen & weiterführende Lektüre

CSA CISO Community / SANS / OWASP / [un]prompted: „The AI Vulnerability Storm: Building a Mythos-ready Security Program", April 2026 (CC BY-NC 4.0) — labs.cloudsecurityalliance.org

Omdia: „The Agentic SOC: SecOps Evolution into Agentic Platforms", 2025 • Microsoft Security Blog: „The Agentic SOC", April 2026 • Torq: Series-D Announcement, Januar 2026 • Brandefense: „Agentic AI in Cybersecurity", 2026 • IDC: Voice of Security 2025 • ReliaQuest Annual Threat Report 2026

**suresecure GmbH**
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

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