

WARUM EINE AGENTIC SOC PLATTFORM?

Mehr Bedrohungen noch schneller erkennen.
Besser entscheiden. Zügig entgegenwirken.

Gartner prognostiziert, dass **40 % der Agentic-AI-Projekte im Jahr 2027 wieder eingestellt werden**. Untersuchungen zu Infrastruktur und Observability zeigen, dass sich diese Fehlschläge insbesondere auf Auto-Remediation und agentengesteuerte Workflows konzentrieren. Mehr als ein Drittel dieser Projekte – **38 % – scheitert an unzureichender Datenverfügbarkeit**.

Dieses Datenproblem wird zunehmend zu einem Sicherheitsproblem. KI ist nur so gut wie die Daten, auf deren Grundlage sie angewandt wird. Fragmentierte, unzureichend gesteuerte oder kontextarme Daten verstärken falsche Alarmer, steigern Risiken und Kosten. Saubere, strukturierte und empirische Daten bilden die Grundlage für ein Agentic SOC Ansatz

WARUM SICH DER SOC VERÄNDERN MUSS

Die meisten Security Operations Center nehmen fälschlicherweise an, dass sie bereits über ausreichende Sichtbarkeit verfügen. Was oft fehlt, ist die Möglichkeit, diese Sichtbarkeit in "True Positives" und in dem Fall schnelle, kontrollierte Gegenmaßnahmen umzuwandeln. Das Datenvolumen wächst kontinuierlich, Angreifer agieren mit KI-Geschwindigkeit und Security-Teams sollen die steigende Zahl der Angriffe sicher abwehren – bei gleichzeitig begrenzten Budgets und Personalressourcen.

Das grundlegende Problem ist struktureller Natur. Das klassische SIEM-zentrierte SOC wurde für Log-Aufbewahrung und Alarmierung entwickelt, nicht für das Treffen von wirksamen Entscheidungen. Plattformen der

nächsten Generation versprochen KI, lieferten jedoch mehr Fehlalarme statt besserer Ergebnisse. Analysten priorisieren weiterhin auf Grundlage ihrer Erfahrung, während Datenvolumen-basierte Preismodelle die Budgets belasten und hybride Multi-Cloud-Umgebungen Teams an ihre Belastungsgrenzen bringen.

Threat-Intelligence-Plattformen wurden für die Bedrohungsanalyse entwickelt, nicht für die operative Umsetzung der Gefahrenabwehr. Automatisierung ohne ausreichenden Kontext erzeugt häufig zusätzliches Rauschen, anstatt Risiken zu reduzieren. Das Ergebnis ist ein SOC, das reaktiv, teuer und inkonsistent bleibt.

Security Operations benötigen deshalb heute eine Intelligence-native Architektur: eine Architektur, die Kontext bereits bei der Datenaufnahme hinzufügt, auf einer KI-fähigen, normalisierten Datenbasis (OCSF) aufsetzt und kontrollierte Reaktionen in Maschinengeschwindigkeit ermöglicht – unter menschlicher Aufsicht.

Die **Anomali Agentic SOC Plattform** vereint einen hochqualitativen Security Data Lake, **Managed Intelligence as a Service (MlaaS)** und echte Agentic AI in einer einheitlichen operativen SOC-Umgebung. Statt weitere Alarmer und Dashboards zu produzieren, verwandelt sie Telemetrie- und Intelligence Daten in durchdachte Entscheidungen mit hoher Zuverlässigkeit.

Dieser Leitfaden erklärt, was eine Agentic SOC Plattform ist, wie sie in der Praxis funktioniert und wie die Kernkomponenten von Anomali zusammenarbeiten, um moderne SOC- und CTI-Teams zu entlasten.

WAS IST EINE AGENTIC SOC PLATTFORM?

Eine Agentic SOC Plattform ist eine operative Sicherheitsplattform, auf der KI-gesteuerte Agenten zusammen mit Analysten arbeiten und eigene Security-Daten sowie externe Threat Intelligence Daten über Machine Learning analysieren, um Detection, Investigation und Response gesamtheitlich in einem Vorgang zu unterstützen.

Im Gegensatz zu klassischen Analyse- oder Automatisierungslösungen arbeitet sie auf der **Entscheidungsebene**. Statt lediglich Alarme zu generieren oder vordefinierte Playbooks auszuführen, analysiert sie kontinuierlich Telemetrie, angereicherte Threat Intelligence und historischen Kontext, um:

- Intelligence-native Detection bereits bei der Datenaufnahme zu ermöglichen
- Alert Noise zu reduzieren und relevante Ereignisse zu priorisieren
- handlungsrelevanten Untersuchungskontext bereitzustellen
- Analysten zu effektiven Reaktionsentscheidungen zu führen
- Übergreifende Threat Intelligence teamübergreifend kontinuierlich zu operationalisieren

Analysten behalten dabei die Kontrolle. Agentic AI sorgt für Geschwindigkeit, Kontext und Konsistenz, und jede autonome Aktion erfolgt innerhalb der vom SOC definierten Governance-Regeln.

Genau darin liegt der Unterschied zwischen einer Plattform, die für geführte Alarmierung entwickelt wurde und einer Plattform, die für Entscheidungen entwickelt wurde.

DAS SECURITY DECISION BRAIN: DREI FÄHIGKEITEN, EIN KONTROLLIERTES SYSTEM

Die meisten SOC's nutzen bereits eine oder zwei dieser Fähigkeiten. Nur wenige betreiben jedoch alle drei als ein integriertes System – und genau diese Lücke führt dazu, dass Untersuchungen ins Stocken geraten und Entscheidungen inkonsistent werden.

Telemetrie, Kontext und Handlung müssen gemeinsam und

unter einem einheitlichen Kontrollrahmen funktionieren. Anomali bezeichnet dieses System als Security Decision Brain.

Alles sehen: Live-Security-Telemetrie und Signale aus eigenen Endpoint, Netzwerk, Cloud, Identity, IT/OT, E-Mail und SaaS systemen angereichert mit externer Thread Intelligence – normalisiert, korreliert und in Echtzeit abfragbar.

Wissen, was relevant ist: Threat Graph, Asset Inventory, User Baselines, Topologie und Incident History werden mit Telemetrie zusammengeführt. Ein Rohsignal zeigt Ihnen, was passiert ist. Kontext zeigt Ihnen, was es für Ihr Unternehmen bedeutet.

Mit Sicherheit handeln: Agentic AI bringt echte Handlungsfähigkeit in das SOC. Statt statischer Dashboards oder reiner Chat-Copilots analysieren Agenten Ihren Data Lake und den Intelligence-Kontext, um Untersuchungen zu unterstützen, nächste Schritte zu empfehlen und Response-Workflows zu automatisieren – weniger Schritte, schnellere Entscheidungen und eine konsistentere Umsetzung.

DIE ANOMALI AGENTIC SOC PLATTFORM

Das Security Decision Brain basiert auf drei integrierten Komponenten. Jede löst ein konkretes operatives Problem – und ihr Mehrwert verstärkt sich, wenn sie zusammenarbeiten.

Rohdaten ohne Intelligence sind Rauschen. Intelligence ohne Daten bleibt Reporting.

1. UNIFIED SECURITY DATA LAKE

Jede SOC-Aktivität ist von Daten abhängig. Wenn Telemetrie unvollständig, verzögert oder deren Indexierungsgrenzen eingeschränkt sind, geraten Securityuntersuchungen ins Stocken und die Qualität von Entscheidungen nimmt ab.

Der Anomali Unified Security Data Lake ist eine moderne, KI-fähige und skalierbare Security-Datenarchitektur, die speziell für Intelligence-getriebene Security Operations entwickelt wurde.

Im Gegensatz zu klassischen SIEM-Data Lakes kann Anomali bestehende SIEM-Investitionen ergänzen, die SIEM-Kosten reduzieren oder ganz ersetzen. Anomali beseitigt Engpässe bei der Datenaufnahme sowie unkalkulierbare Datenvolumenkosten.

WAS ES IST	WAS ES LEISTET
Unified Security Data Lake	Vollständige und harmonisierte-Telemetrie aus Cloud, Endpoint, Netzwerk, Identity, IT/OT und externen Quellen. Jederzeit verfügbar und für KI-Systeme verständlich – ohne die Kosten- oder Performance-Grenzen klassischer SIEM-Systeme.
Managed Intelligence as a Service (MlaaS), powered by ThreatStream Next-Gen	Echtzeitkontext, auf den eine KI-Architektur angewiesen ist. Der Data Lake wird kontinuierlich mit aktuellen Informationen zu Threat Actors, TTPs und Kampagnen angereichert und operationalisiert Threat Intelligence innerhalb von Minuten statt erst nach mehreren Arbeitstagen.
Agentic AI	Eine mit KI bewerte Wichtigkeit und nach Prioritäten geordnete Entscheidungs-Queue, MCP-fähige agentische Security Operations sowie Tier-1- und Tier-2-Triage-Agenten, die die Entscheidungslogik Ihres SOC widerspiegeln – anstatt starren, vom Anbieter vorgegebenen Runbooks zu folgen

Er bietet:

- zentrale Aufnahme von Security-Telemetrie aus Cloud-, Endpoint-, Netzwerk-, Identity-, IT/OT- und Applikationsquellen
- Security-native Normalisierung und Korrelation bereits bei der Datenaufnahme in OCSF
- dauerhaft durchsuchbare und untersuchungsbereite Daten ohne Kompromisse bei der Speicherung
- Hochgeschwindigkeitssuche und Analytics über Monate oder Jahre innerhalb von Threat Intelligence- und Telemetriedaten

Da Telemetrie bereits bei der Aufnahme normalisiert und korreliert wird, arbeiten alle nachgelagerten Prozesse mit sauberem und konsistentem Kontext. Analysten und Agentic AI können schnell zwischen Alerts, Artefakten und Zeitlinien wechseln – ohne tote Winkel.

Dabei handelt es sich nicht um Cold Storage. Die Daten sind jederzeit verfügbar und durchsuchbar – sowohl für Echtzeit- als auch für historische Analysen.

2. MANAGED INTELLIGENCE AS A SERVICE (MIAAS), POWERED BY THREATSTREAM NEXT-GEN

Die beste Telemetrie allein zeigt noch kein Risiko auf. Zu wissen, dass etwas passiert ist, ist nicht dasselbe wie zu wissen, was genau zu erwarten ist, wer dahintersteckt,

warum es jetzt relevant ist oder was als nächstes im weiteren Angriffsverlauf passieren könnte.

Managed Intelligence as a Service (MlaaS), powered by ThreatStream Next-Gen, bildet eine zusätzlichen Entscheidungslayer eines Agentic SOC und unterstützt gleichzeitig die bestehende Sicherheitsarchitektur, auf der das jeweilige SOC aufbaut.

MlaaS reichert den Security Data Lake kontinuierlich mit valider und bereinigter Threat Intelligence an, die dazu mit KI berechneten Confidence Scores versehen wird:

- Threat Actors, Kampagnen und Infrastruktur
- Taktiken, Techniken und Verfahren, die MITRE ATT&CK zugeordnet sind
- Behavioral Context und Indicator-of-Attack-Context
- Asset-basierter Kontext in Verbindung mit dem organisatorischen Risiko

Statt Threat Intelligence statisch bereitzustellen, wird sie stetig mit interner Telemetrie korreliert. Dadurch begleitet der Kontext jeden Alert, jede Untersuchung und wird innerhalb von Minuten operationalisiert – statt erst nach mehreren Stunden oder Arbeitstagen.

SOC- und CTI-Teams können dadurch Bedrohungen auf Grundlage der Absicht des Angreifers und ihrer operativen Relevanz zügig priorisieren, statt nur nach der Menge von Indikatoren zu entscheiden.

3. AGENTIC AI

Agentic AI unterstützt SOC-Teams über die verbesserte Daten- und Intelligence-Schicht – genau dort, wo gute Entscheidungen zügig getroffen werden müssen.

Zu den Funktionen gehören:

- automatisierte Anreicherung und Untersuchung von Alerts
- Behavioral- und regelbasierte Analysen mit Fokus auf die Absicht des Angreifers
- Intelligence-basierte Handlungsempfehlungen direkt in Alerts und Cases
- kontextbezogene Response- und Mitigation-Empfehlungen
- semantische Suche und Interaktion in natürlicher Sprache auf Grundlage von Security-Kontext

Die KI-gesteuerten Agenten von Anomali analysieren den Unified Security Data Lake und die Intelligence aus MlaaS, um Investigation und Response zu unterstützen.

Dabei spiegeln sie die Entscheidungslogik Ihres SOC individuell wider, statt auf starren Workflows eines SOAR-Anbieters zu basieren. Sie reduzieren manuellen Aufwand und Inkonsistenzen und unterstützen Analysten bei Ihren Entscheidungen.

Analysten verbringen dadurch weniger Zeit mit der manuellen Korrelation von Daten und mehr Zeit mit Bewertung des Kontextes und zeitnaher Handlung, im besten Fall kommen sie vor die Lage.

WIE AGENTIC SOC OPERATIONS FUNKTIONIEREN

Eine Agentic SOC Plattform lässt sich am besten verstehen, wenn man betrachtet, wie sie im täglichen Betrieb arbeitet.

So greifen Detection, Investigation und Response innerhalb der Anomali Agentic SOC Plattform ineinander.

DETECTION: VOM SIGNAL ZUM KONTEXT

Detection beginnt damit, dass Telemetriedaten in den Unified Security Data Lake fließen. Da die Daten nahezu in Echtzeit normalisiert und angereichert werden, basieren Detections auf vollständigen und unveränderten Daten – statt auf stichprobenartigen oder verzögerten Logs.

MlaaS reichert diese Telemetrie kontinuierlich mit

realer Threat Intelligence an. Agentic AI bewertet Alerts anschließend anhand historischer Muster, Behavioral Context und Adversary Intelligence, um Signale mit geringer Relevanz zu unterdrücken und Bedrohungen mit hoher Zutrefflichkeit hervorzuheben.

INVESTIGATION: KONTEXT OHNE MANUELLE KORRELATION

Wenn ein Alert eskaliert wird, korreliert Agentic AI automatisch:

- zusammenhängende Entitäten und historische Aktivitäten
- Threat Actors, Kampagnen und Infrastruktur
- Behavioral Indicators, die mit den TTPs des Angreifers übereinstimmen

Analysten können mithilfe semantischer Suche und spezieller Investigation Workbenches zwischen Indikatoren, Zeitlinien und Threat Models wechseln.

Knowledge Graphs verbinden Abfragen in natürlicher Sprache mit strukturierten Security-Daten. Dadurch wird mehrstufiges Reasoning möglich, ohne dass Analysten komplexe Abfragen erstellen müssen.

RESPONSE: GEFÜHRTE UND KONTROLLIERTE HANDLUNGEN

Agentic AI liefert kontextbezogene Response-Empfehlungen, die auf das konkrete Threat-Szenario und die jeweilige Umgebung abgestimmt sind und durch Intelligence, Telemetrie und frühere Ergebnisse unterstützt werden.

Dadurch werden Unsicherheit und unterschiedliche Vorgehensweisen reduziert.

Da Threat Intelligence und Kontext über den gesamten Prozess hinweg eingebettet sind, kann Response konsistent über SOC, CTI und nachgelagerte Systeme ausgeführt werden, darunter SOAR, EDR, XDR und Ticketing-Systeme.

Response wird dadurch **konsistent, entscheidungsbasiert, kontrolliert und effizient**.

MESSBARE ERGEBNISSE

Unternehmen führen eine Agentic SOC Plattform ein, um operative Ergebnisse zu verbessern– nicht, um einzelne Tools geringfügig zu verbessern.

Anomali hat folgende Zielwerte mehrfach gemessen:

MENGE	ERGEBNIS
30–50 %	Reduzierung der Total Cost of Ownership
90 %	Reduzierung kritischer Incidents
60–70 %	Analystenzeit, die durch die Reduzierung der False-Positive-Triage zurückgewonnen wird

WIE DIE PLATTFORM ALS SYSTEM FUNKTIONIERT

Das entscheidende Merkmal einer Agentic SOC Plattform ist das Zusammenspiel ihrer Komponenten:

- Der **Unified Security Data Lake** hält Telemetriedaten vollständig, verfügbar und normalisiert.
- **MlaaS, powered by ThreatStream Next-Gen**, verwandelt Threat Intelligence in operativen Kontext.
- **Agentic AI** analysiert beide Ebenen und unterstützt Detection, Investigation und Response.

Dieser integrierte Ansatz reduziert Tools sowie manuelle Übergaben und spart Budget ein.

Threat Intelligence ist nicht länger vom operativen Betrieb getrennt und KI wird nicht einfach nachträglich auf bestehende Systeme aufgesetzt.

Die Plattform funktioniert als eine einheitliche operative Ebene, auf der Daten, Intelligence und Entscheidungen miteinander verbunden bleiben.

WAS ANOMALI OPTIMIERT

Das Security-Problem ist heute zunehmend ein Prozess und Datenproblem. Kontext, Intelligence und kontrollierte Autonomie müssen auf einer einheitlichen Datenschicht zusammenarbeiten.

- **Ein konsolidierter Data Lake:** ein Jahrzehnt kuratierter Intelligence kombiniert mit einer Topologie menschlicher und nicht-menschlicher Identitäten.
- **Operationalisierte Managed Intelligence:** kontextbasierte Entscheidungen über das gesamte Security-Ökosystem hinweg steuern.
- **Eine einheitliche Plattform ohne Konzentrationsrisiko:** herstellerneutral und architekturunabhängig, sodass sie mit den bereits eingesetzten Tools zusammenarbeitet.

AGENTIC AI IN SECURITY OPERATIONS OPERATIONALISIEREN

Eine Agentic SOC Plattform verändert grundlegend, wie Security Operations aufgebaut sind.

Statt einzelne Tools zu optimieren, ermöglicht sie bessere Entscheidungen und entwickelt den SOC von einem reaktiven Alert Center zu einer **Intelligence-nativen, KI-beschleunigten Decision Engine**.

Die Anomali Agentic SOC Plattform vereint kontinuierlich verfügbare Telemetrie, laufend angereicherte Threat Intelligence und Agentic AI.

Damit können Unternehmen:

- modernisieren, ohne disruptive Rip-and-Replace-Projekte
- bestehende SIEM-Investitionen ergänzen oder ersetzen
- Kosten und Komplexität erheblich reduzieren
- auf KI-gesteuerte Angreifer vorbereitet sein
- Security Operations über hybride Multi-Cloud-Umgebungen hinweg optimieren

Für Teams, die sich von Alert-zentrierten Security Operations lösen wollen, bietet die Plattform einen praktischen Weg zu prädiktiven Handlungen.

Im Fokus stehen dabei:

- schnellere Detection und Triage durch Intelligence-basierte Priorisierung

- kürzere Untersuchungszyklen dank vollständigem historischen und Angreiferkontext
- weniger Alert Fatigue und Analyst Burnout
- konsistentere und wiederholbare Security-Entscheidungen über Teams hinweg
- stärkere Abstimmung zwischen SOC und CTI

Diese Ergebnisse entstehen dadurch, dass die Plattform Rohdaten bis hin zur geführten Handlung weiterverarbeitet – statt bei Alerts oder Analytics stehenzubleiben.

**ALLES SEHEN.
WISSEN, WAS RELEVANT IST.
MIT SICHERHEIT HANDELN.**

ANOMALI IN AKTION ERLEBEN
[Demo anfordern](#)