AMC SOC

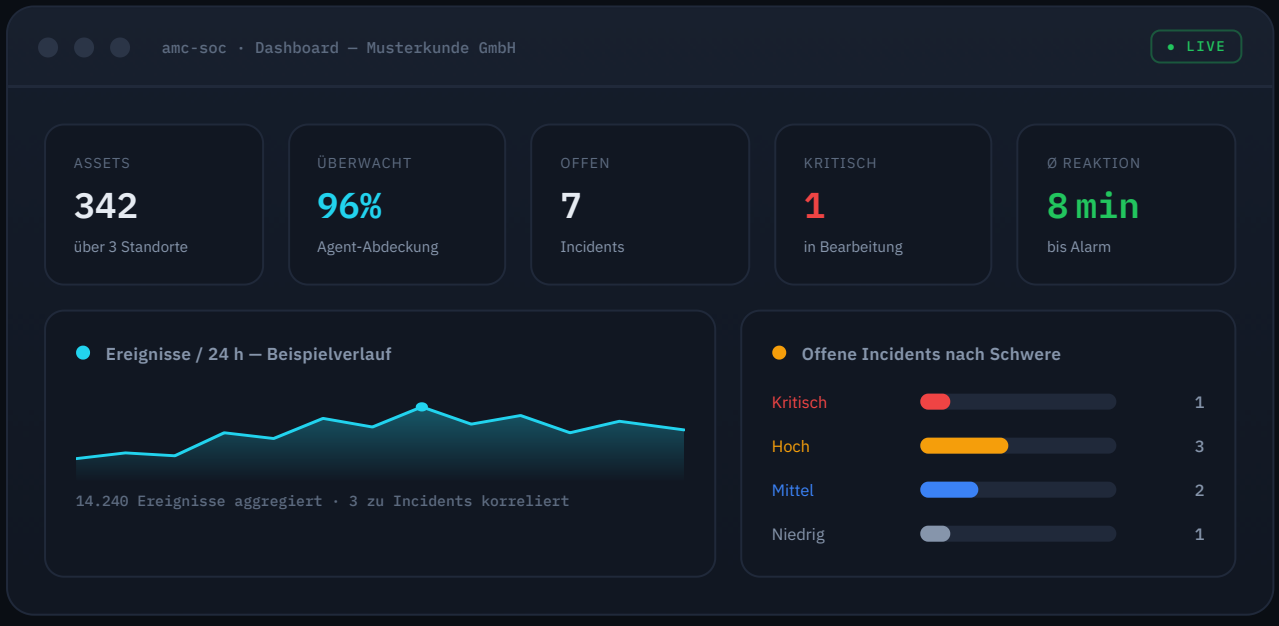
AMC IT SERVICES GMBH · SECURITY OPERATIONS

MANAGED SECURITY OPERATIONS CENTER

Ihre IT wird rund um die Uhr überwacht. Ganz ohne eigenes SOC-Team.

Angriffe laufen 24/7 — Ihr Team nicht. AMC SOC bündelt Endpunkte, Netzwerk, Schwachstellen und Firewall an einem Ort, erkennt Bedrohungen automatisch und meldet sie klar priorisiert. Betrieben von AMC IT Services, on-premises, DSGVO-konform.

- Rundum-Überwachung 24/7
- On-Prem & DSGVO
- Managed & reaktionsschnell
- In Tagen einsatzbereit



Beispielansicht mit Musterdaten — keine echten Kundendaten.

WARUM AMC SOC

Sicherheit als Service — statt Feuerwehr im Ernstfall.

Die meisten Angriffe scheitern nicht an fehlender Technik, sondern daran, dass niemand rechtzeitig hinschaut. AMC SOC übernimmt genau das: kontinuierlich, nachvollziehbar, und ohne dass Sie ein eigenes Security-Team aufbauen müssen.

Rundum-Überwachung, 24/7

Endpunkte, Netzwerkverkehr, Schwachstellen und Firewall laufen in einem gemeinsamen Lagebild zusammen. Auffälligkeiten werden automatisch korreliert und priorisiert — Tag und Nacht, auch an Wochenenden.

On-Prem & DSGVO-konform

Ihre Daten bleiben im Haus. Die Analyse — inklusive der KI-Auswertung — läuft lokal auf AMC-Infrastruktur, ohne Versand an Cloud-Dienste Dritter. Ein deutscher Partner, klare Verantwortlichkeiten.

Managed & reaktionsschnell

Aus erkannten Bedrohungen werden automatisch nachvollziehbare Vorfälle und Tickets — mit Handlungsempfehlung und, wo freigegeben, direkter Reaktion (z. B. Sperre am Perimeter). Sie behalten die Kontrolle, wir die Wachsamkeit.

In Tagen einsatzbereit

Eine vorkonfigurierte Sensor-Appliance und ein automatischer Agent-Rollout per Gruppenrichtlinie bringen Ihre Umgebung in Tagen unter Überwachung — nicht in Monaten, und ohne aufwändiges Projekt.

WAS WIR ÜBERWACHEN

Eine Plattform. Alle sicherheitsrelevanten Quellen.

Für die IT-Abteilung: AMC SOC vereint etablierte Open-Source- und Enterprise-Sensorik unter einem Dach. Jede Quelle speist denselben Data Lake — Korrelation über Quellgrenzen hinweg, statt Insellösungen.

Endpunkt-Sicherheit

Agent-basiert · Host-Telemetrie

Logs, Dateiintegrität, Schwachstellen und angemeldete Benutzer je Host — Windows, Linux, Server.

Netzwerk-Erkennung

IDS · Metadaten · Flows

Signaturbasierte Erkennung, Protokoll-Metadaten und Verbindungsflüsse — vom Exploit-Versuch bis zum auffälligen Datenabfluss.

Schwachstellen-Scan

authentifiziert & unauth.

Regelmäßige, selbstgesteuerte Scans im Kundennetz mit tagesaktuellem Feed → priorisiertes Schwachstellen-Center.

Perimeter & Firewall

Firewall-Integration

Blockierte und erlaubte Verbindungen, wiederkehrende Scanner — mit optionaler, reversibler Sperre.

Endpoint-Forensik

DFIR · auf Anforderung

Auf Anforderung: Prozesse, Autostarts, Netzverbindungen — und reversible Isolation im Ernstfall.

KI-Analyst

lokal ausgewertet · on-prem

Fasst jeden Vorfall verständlich zusammen, bewertet Schwere und nennt konkrete Maßnahmen — ohne Cloud-Versand.

Täuschung & Discovery

Deception · Netzwerk-Scan

Köder-Dienste schlagen bei jeder Berührung an; neue, unbekannte Geräte im Netz fallen sofort auf.

AV / EDR-Status

herstellerübergreifend

Ist der Virenschutz überall aktiv und aktuell? Schutzlücken werden erkannt, bevor sie ausgenutzt werden.

Verzeichnis & Konten

Verzeichnisdienst

Privileg-Änderungen, verwaiste Admin-Konten und Abdeckungslücken — der Blick aufs Wer.

INC-0287 **Verdächtige Kontenänderung an Domänencontroller** KRITISCH · 92 T1078 T1098 SRV-MUSTER-DC01

KI-ANALYSE · LOKAL AUSGEWERTET

Ein Benutzerkonto wurde außerhalb der Geschäftszeiten der Gruppe „Domänen-Admins" hinzugefügt, kurz nach mehreren fehlgeschlagenen Anmeldungen von derselben Quelle. Muster deutet auf Rechteausweitung nach kompromittiertem Zugang hin. Empfohlen: sofortige Prüfung des Kontos.

- → Neu hinzugefügtes Admin-Konto verifizieren und bei Bedarf entfernen
- → Quell-IP der Fehlversuche am Perimeter sperren (reversibel, befristet)
- → Betroffenen Host per Endpoint-Forensik triagieren

Beispiel-Vorfall mit Musterdaten – dient nur der Illustration.

SO LÄUFT ES

Vom Rollout zum Alarm — in vier Schritten.

Kein Monatsprojekt: Sie bekommen eine fertige Sensor-Appliance und rollen die Agenten automatisiert aus. Ab dann arbeitet AMC SOC im Hintergrund.

01 · Onboarding

Sensor & Agenten

Vorkonfigurierte Appliance ins Netz, Agenten per Gruppenrichtlinie still auf alle Rechner.

→

02 · Erfassung

Data Lake

Alle Quellen speisen ein gemeinsames Lagebild — Endpunkt, Netz, Schwachstellen, Firewall.

→

03 · Analyse

Korrelation & KI

Regeln verknüpfen Ereignisse quellenübergreifend; die lokale KI bewertet und erklärt.

→

04 · Reaktion

Incident & Ticket

Priorisierter Vorfall mit Empfehlung, automatischem Ticket und — auf Wunsch — direkter Sperre.

Mandantenfähig · Daten je Kunde getrennt

Reversibel · keine Blind-Aktionen ohne Freigabe

Nachvollziehbar · lückenloses Audit

Datenehrlich · Quellenausfall wird gemeldet, nie beschönigt

BEREIT, RUHIGER ZU SCHLAFEN?

Lassen Sie uns Ihre Umgebung gemeinsam absichern.

Wir zeigen Ihnen AMC SOC an einer Beispielumgebung und erstellen ein passendes Angebot für Ihre Standorte und Geräteanzahl.

Demo & Angebot anfragen

TELEFON
06188-4479644

E-MAIL
office@amc-it-services.de

WEB
www.amc-it-services.de

ANBIETER
AMC IT Services GmbH

Alle Ansichten & Kennzahlen sind Musterdaten.