SOC & MDR

Der ultimative Leitfaden

WHITEPAPER

sure[secure] X securance

Einleitung

Die frühzeitige Erkennung von Cyberangriffen ist eine zentrale Säule im Rahmen der Prävention. Je eher ich einen Angriff identifiziere, desto eher habe ich die Möglichkeit, entsprechend darauf zu reagieren. Dadurch wird das Risiko reduziert. Doch wie werden Cyberangriffe denn idealerweise frühzeitig erkannt? Welche Begriffe in diesem Kontext immer wieder genannt werden:

- Security Operations Center
- Managed Detection and Response

Beide Buzzwords können einen erheblichen Beitrag dazu leisten und somit eine wichtige Rolle im Rahmen der Cyber-Resilienz einnehmen. Beides wird in der Regel als Service angeboten und beide sind darauf ausgelegt, Sicherheitsbedrohungen zu Identifizierung und darauf zu reagieren. Beides sind zudem keine klar definierten Begriffe, weshalb es immer wichtig ist, auf die Details zu achten. Manche bezeichnen ein MDR als SOC oder betreiben ein SOC ohne SIEM-Lösung.

Es ist also wichtig, die Unterschiede zu verstehen, um die richtige Wahl zu treffen und die Angebote auf dem Markt genau prüfen zu können. Hier also der ultimative Leitfaden.

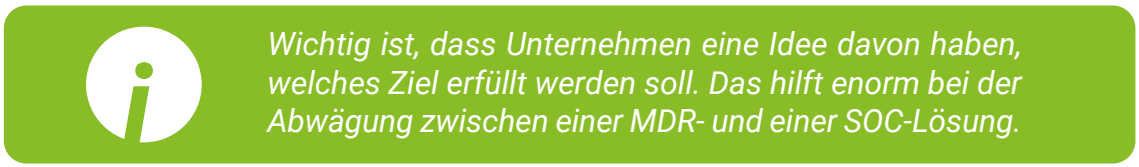
Welches Kernproblem muss denn gelöst werden?

Unternehmen stehen vor mehreren Herausforderungen, wenn es darum geht, eine durchgehende Früherkennung von Cyberbedrohungen zu etablieren.

Moderne IT-Umgebungen sind oft komplex und umfassen eine Vielzahl von Assets wie Endgeräten, Netzwerken oder Cloud-Diensten. Nehmen wir die Schatten-IT der Unternehmen hinzu, ergibt sich schnell ein unübersichtliches Bild. Dadurch wird es schwierig, alle potenziellen Einfallstore und Angriffsvektoren zu überwachen. Es gibt zu viele Blind-Spots und nicht gemanagte Systeme.

Das liegt mitunter auch daran, dass die Unternehmen Schwierigkeiten haben, Fachkräfte zu finden, die eben genau hier Abhilfe schaffen. Das trifft zum einen auf die allgemeine IT-Sicherheit zu und wird nochmals schwieriger, wenn es darum geht, z. B. ein eigenes SOC aufzubauen. Nur diese Fachkräfte sind in der Lage, die Verarbeitung und die Analyse solch großer Mengen von Security-Events durchzuführen und zu erkennen, welche Alerts nun wirklich die Aufmerksamkeit von Analysten verdienen.

Deshalb evaluieren Unternehmen verstärkt Service-Provider, um das Unternehmen vor dem größten Geschäftsrisiko der Welt zu bewahren. Doch anhand welcher Kriterien geht man hier vor? Was wird wirklich benötigt?



SOC & MDR – Unterschiede und Gemeinsamkeiten

Die Gemeinsamkeiten sind in diesem Falle recht offensichtlich und etwas anderes macht auch wenig Sinn. Denn diese bilden die Grundvoraussetzung dafür, dass das Ziel einer durchgehenden Überwachung erfüllt werden kann.

- **24x7 Überwachung:**
  Ohne geht es nicht, denn Cyberkriminelle nutzen besonders gerne die Zeitfenster, wo wissentlich niemand mehr im Büro sitzt.
- **Bedrohungsanalyse:**
  Sowohl SOCs als auch MDR-Dienste analysieren Bedrohungsdaten und nutzen moderne Technologien wie maschinelles Lernen und auch Komponenten mit AI-Unterstützung.
- **Incident Response:**
  Ganz entscheidend ist doch, was wird eigentlich getan, wenn etwas Verdächtiges identifiziert wird? Reagieren und mitigieren müssen deshalb in beiden Services auftauchen. Wichtig sind hier insbesondere die SLA-Zeiten – also in welchem Zeitrahmen geschieht hier eine erste Reaktion.
- **Geschwindigkeit:**
  In der Cloud-Variante sind beide Services sehr schnell bereitgestellt und unterstützen die IT-Abteilung innerhalb weniger Tage mit dem vollen Umfang.

Schauen wir uns aber weitere Kriterien an, werden Unterschiede erkennbar, auf die wir im weiteren Verlauf näher eingehen werden. Hier eine Gegenüberstellung wichtiger Faktoren von MDR- und SOC-Service.

Kriterium	Managed SOC	MDR
Ressourcen	Extern	Extern
Anpassungsfähigkeit	Hoch	Mittel
Kosten	Variable Kosten (abhängig von Volumen/Nutzer oder Assets)	Variable Kosten
Implementierungszeit	Kurz (Cloud based) Mittel (On-Prem)	Kurz (Cloud based) Mittel (On-Prem)
Fachwissen	Externes, hochspezialisiertes Fachwissen	Externes, hochspezialisiertes Fachwissen
Skalierbarkeit	Hoch	Hoch
Fokus	Frühzeitige Erkennung auch komplexer Angriffe sowie schnelle Reaktion darauf	Erkennung und schnelle Reaktion auf Bedrohungen
Sicherheitsmaßnahmen	Umfassend, inkl. Prävention, Korrelation, Erkennung und Reaktion auf Alerts	Erkennung und Reaktion auf Alerts
Log-Quellen	On-Prem & Log-Quellen möglich	Limitierte Möglichkeiten in Abhängigkeit zum Hersteller
Eingesetzte Technologien	SIEM, SOAR, IDS/IPS, EDR, Schwachstellenscanner plus spezialisierte Tools des Anbieters	EDR, MDR-spezifische Plattformen (z.B. auch SOAR)
Verfügbarkeit	24x7	24x7 (wird teilweise auch als 10x5 o. Ä. angeboten, was allerdings wenig Sinn macht)

Bevor wir zu den wichtigen Unterschieden kommen, ist es wichtig zu verstehen, dass beide Services extern gemanagt werden. D. h. es müssen beim Anbieter Expert:innen sitzen, die mit Erfahrung und Leidenschaft Alerts analysieren und schnell die richtigen Rückmeldungen geben. Dies sollte dringend in der Evaluierung berücksichtigt werden.

Bei einem SOC-Service geht es um deutlich mehr Komplexität im positiven Sinne. Denn die Korrelation kann ein echter Gamechanger in der Identifizierung von Anomalien sein. Ein Beispiel:

Der MDR-Service erkennt, dass Zugriffe von einem Notebook an einem Sonntag erfolgen. Dies wird in Zeiten von Remote-Work und Home-Office gerne als False-Positives bezeichnet. Was aber, wenn der Zugriff vom Notebook aus einem anderen Land erfolgt ist und plötzlich eine erhöhte Netzwerkauslastung bemerkt wird?

Die einzelnen Faktoren mögen unbedeutend erscheinen, doch das Zusammenfügen der Datenstränge offenbart eine ganz andere, umfassende Geschichte.

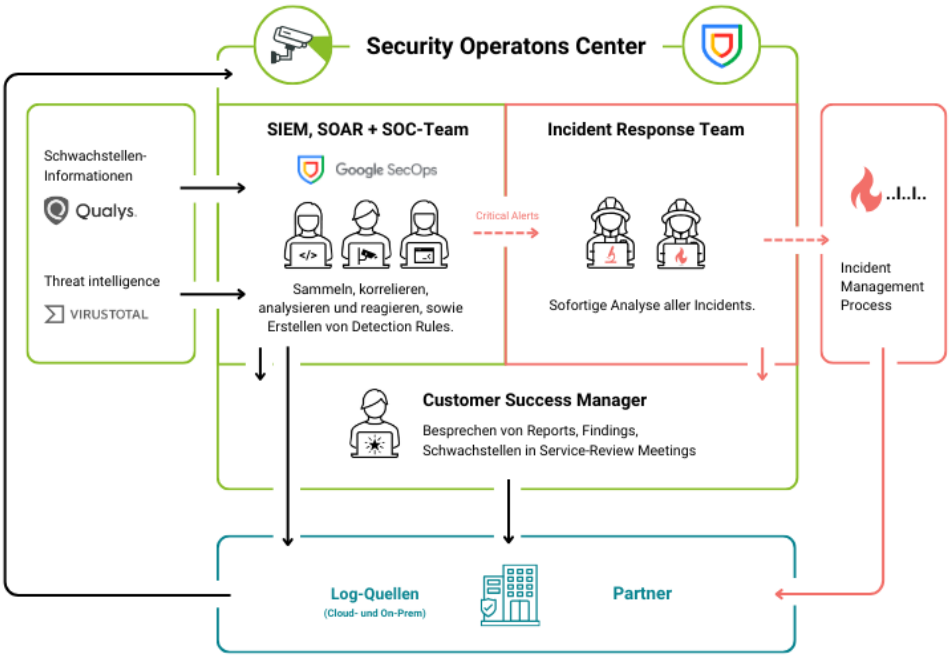


Schaubild: SOC @ SURESECURE

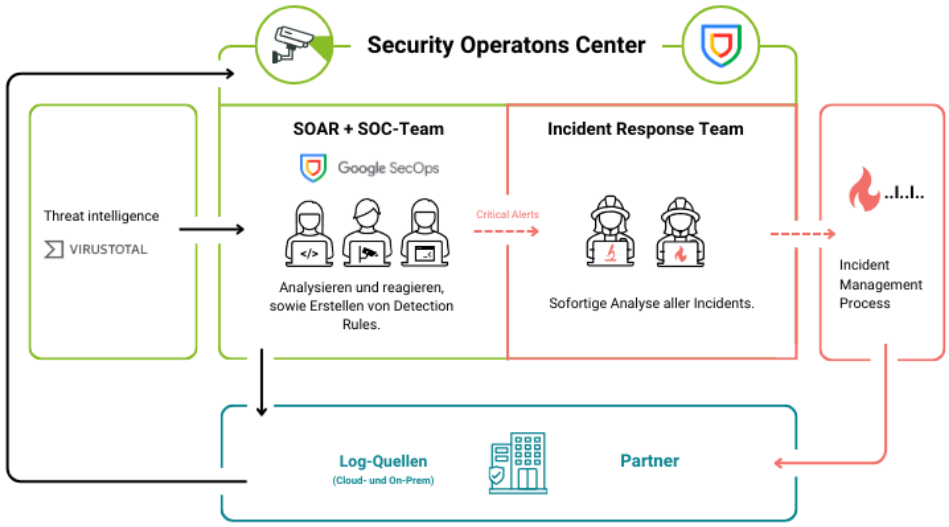


Schaubild: MDR @ SURESECURE

Das funktioniert nur, wenn auch entsprechende Technologien eingesetzt werden. So basieren MDR-Services häufig auf EDR-Systemen oder verarbeiten die Daten von EDR-Systemen, wo SOC-Services in der Regel ein SIEM, SOAR, IPS/IDS, Schwachstellenscanner und weitere Tools beinhalten, um einen möglichst umfangreichen Überblick zu erhalten.

Mythen und Fabelgeschichten über SOC und MDR

Ein SOC ist nur für große, ein MDR nur für kleine Unternehmen geeignet. Falsch!

Es gibt die viel verbreitete Annahme, dass ein SOC nur für große Unternehmen mit umfangreichen Ressourcen sinnvoll ist. Diese Annahme entstand in einer Zeit, wo Managed SOCs noch gar kein Thema waren. Sie bezieht sich also auf den Aufbau eines eigenen, internen SOCs. Mittlerweile sind die SOC-Services als Managed Service zu beziehen, wodurch die Einstiegshürde deutlich reduziert wird.

Darüber hinaus glauben viele, dass MDR-Dienste nur für kleine Unternehmen geeignet sind, die keine eigenen Sicherheitsressourcen haben. In Wirklichkeit profitieren Unternehmen jeder Größe von MDR-Diensten, da sie spezialisierte Expertise und fortschrittliche Bedrohungserkennungsfähigkeiten bieten, die auch große Unternehmen unterstützen können.

Ein SOC kann nur Vorfälle erkennen, aber nicht darauf reagieren. MDR-Dienste sind nur reaktiv und nicht proaktiv. Beides falsch!

Dieser Mythos ignoriert die Tatsache, dass ein gut konzipiertes und betriebenes SOC nicht nur Bedrohungen erkennen, sondern auch aktiv darauf reagieren kann. SOC-Teams sind oft mit Incident-Response-Fähigkeiten ausgestattet und können Sofortmaßnahmen ergreifen, um Bedrohungen zu neutralisieren und Schäden zu minimieren.

MDR-Dienste sind nicht reaktiv, sondern umfassen tatsächlich proaktive Bedrohungsanalysen (Threat Hunting), Schwachstellenanalysen und Sicherheitsbewertungen, um potenzielle Bedrohungen zu identifizieren und zu verhindern, bevor sie zu Vorfällen werden.

Ein SOC löst sofort alle Sicherheitsprobleme. MDR-Dienste können alle Bedrohungen erkennen und stoppen. Auch falsch!

Ein SOC ist ein mächtiges Werkzeug zur Erkennung und Reaktion auf Sicherheitsvorfälle, aber es ist kein Allheilmittel. Denn die Effektivität eines SOC hängt stark von den implementierten Prozessen, den Fähigkeiten des Personals und der kontinuierlichen Anpassung an neue Bedrohungen ab. Ohne regelmäßige Updates der Detection Rules wird ein SOC auch schnell ineffizient. Zudem kann es nur das analysieren, was auch angebunden ist.

Es besteht darüber hinaus die falsche Vorstellung, dass MDR-Dienste alle Bedrohungen automatisch erkennen und stoppen können. Obwohl MDR-Dienste fortschrittliche Technologien und Fachwissen nutzen, gibt es keine 100%ige Sicherheit.

SOC und MDR – alles Standardlösungen. Falsch!

Es gibt wohl kaum Services, die so heterogen am Markt platziert werden. Sowohl beim SOC als auch beim MDR steckt die Leistungsfähigkeit in den Service-Level-Agreements. Diese müssen intensiv geprüft werden, um sicherzugehen, dass die Anforderungen auch erfüllt werden. Es gibt SOC-Provider, die z. B. individuelle Detection Rules erstellen oder MDR-Provider, die sich bereits über eine 24x7 Verfügbarkeit differenzieren.

Was wir nun empfehlen? Definitiv frühzeitig professionell beraten lassen.

Die Wahl zwischen einem Managed SOC und MDR hängt stark von den spezifischen Bedürfnissen, Ressourcen und Zielen eines Unternehmens ab.

Externes SOC bietet Flexibilität und Zugang zu Expertenwissen mit variablen Kosten. Es kann umfassende Sicherheitsmaßnahmen und Anpassungsmöglichkeiten bieten, wobei es besonders für Unternehmen vorteilhaft ist, die keine umfangreichen internen Ressourcen aufbauen können oder wollen.

MDR bietet eine schnelle und kosteneffiziente Lösung mit einem starken Fokus auf Erkennung und Reaktion. MDR-Dienste sind besonders attraktiv für Unternehmen ohne umfangreiche interne Ressourcen, da sie spezialisiertes Fachwissen und moderne Bedrohungserkennungstechnologien nutzen, um Bedrohungen effektiv zu erkennen und darauf zu reagieren.

Bei beiden Varianten sollten moderne Best-Practice-Technologien eingebunden sein, um die Sicherheit zu gewährleisten, wobei der Einsatz und die Integration dieser Technologien je nach spezifischen Anforderungen und Ressourcen des Unternehmens variieren können.

Wir freuen uns auf deinen Anruf.

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

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