# Leitfaden für den Kauf von Managed Security

Insight

# Einleitung

Jeder ist sich der Bedeutung der Cybersicherheit bewusst, von CEOs und Vorstandsmitgliedern bis hin zu Privatpersonen. Es vergeht kaum ein Tag, an dem in den Nachrichten nicht über eine große Marke berichtet wird, bei der eine Sicherheitslücke aufgetreten ist, oder über einen Vorfall mit Phishing-E-Mails. Das Internet ist für so viele Bereiche unseres geschäftlichen und privaten Lebens von entscheidender Bedeutung, und der globale Charakter des Internets setzt uns auch einer Reihe globaler Risiken aus.

**Wenn die „Kosten der Internetkriminalität“ ein Land wären, wäre es mit 9 Mrd. USD im Jahr 2024 nach den USA und China die drittgrößte Volkswirtschaft der Welt[1].**

Wir leben in einer Zeit geopolitischer Spannungen und hybrider Kriege. Konflikte werden nicht mehr nur auf dem Schlachtfeld ausgetragen – Nationalstaaten und mit dem Staat verbündete Akteure nutzen regelmäßig Störungen in unserer digitalen Welt, um ihre Ziele in der realen Welt durchzusetzen. Organisierte Verbrecherbanden haben auf Hightech umgestellt und erkannt, dass sich mit Ransomware-Angriffen ein riesiges Vermögen machen lässt - leider mit geringen Chancen, vor Gericht gestellt zu werden.

**In etwa 45% der diesjährigen Fälle exfiltrierten die Angreifer die Daten innerhalb eines Tages nach der Kompromittierung[2].**

Das regulatorische Umfeld war noch nie so streng wie heute - die Europäische Union hat Gesetze wie NIS2 und DORA eingeführt, die Unternehmen dazu verpflichten, ihre Cybersicherheit zu verbessern.

Wir hoffen, dass dieser Leitfaden dazu beiträgt, den Fachjargon zu entschlüsseln und Ihnen einen pragmatischen Wegweiser bietet, wie Sie Ihr Unternehmen durch diese turbulenten Zeiten führen können.

**Bei den nicht erpresserischen Vorfällen in den Jahren 2022 und 2023 blieb die durchschnittliche Zeit bis zur Datenexfiltration durchweg unter einem Tag, was bedeutet, dass die Verteidiger innerhalb von 24 Stunden auf einen Lösegeldangriff reagieren müssen[3].**

# Die Risiken des Nichtstuns

Das Versäumnis, in eine solide Cybersicherheit zu investieren, kann schwerwiegende Folgen haben:

- **Finanzieller Schaden:** Datenschutzverletzungen und Ransomware-Angriffe können Geldstrafen, Rechtskosten und Umsatzeinbußen nach sich ziehen.
- **Reputationsschaden:** Ein Sicherheitsvorfall kann das Vertrauen von Kunden und Stakeholdern erschüttern.
- **Betriebsunterbrechungen:** Cyberangriffe stören häufig Geschäftsprozesse, was zu Verzögerungen und Produktivitätsverlusten führt.
- **Regulatorische Sanktionen:** Die Nichteinhaltung von Rahmenbedingungen wie NIS2 oder DSGVO kann zu erheblichen Bußgeldern führen.

Es ist klar, dass zu geringe Investitionen in die Sicherheit mit offensichtlichen Risiken verbunden sind, aber zu hohe Investitionen oder in die falschen Bereiche sind ebenfalls schlecht für das Geschäft. Zu viel Sicherheit kann zu Frustration bei Mitarbeitern und Kunden führen, ganz zu schweigen von den Opportunitätskosten, die durch den Einsatz dieses Budgets für das Wachstum Ihres Unternehmens entstehen.

Sicherheit ist immer ein Balanceakt. Ziel ist es, „gerade genug“ Sicherheit zu erreichen, ohne andere Auswirkungen auf Ihr Unternehmen zu haben.

# Die Grundlagen verstehen

In der Branche wird eine verwirrende Vielzahl von Abkürzungen verwendet. Das Marketing der Anbieter trägt dabei erheblich zur Verwirrung bei. Es lohnt sich, einige der gebräuchlichsten zu kennen und zu verstehen, um sicherzustellen, dass Sie mit Lieferanten und Partnern dieselbe Sprache sprechen.

## Technologie:

- **Microsoft Defender for Endpoint to deliver (MEDR):** Konzentriert sich auf die Identifizierung und Reaktion auf Bedrohungen für einzelne Endpunkte/-geräte (Laptops, Server, mobile Geräte) durch die Bereitstellung detaillierter forensischer Daten und Abhilfemaßnahmen.
- **Network Detection and Response (NDR):** ist ein Cybersicherheitsansatz, der fortschrittliche Analysen, maschinelles Lernen und Verhaltenserkennung einsetzt, um den Netzwerkverkehr in Echtzeit zu überwachen, Anomalien oder Bedrohungen zu erkennen und verwertbare Erkenntnisse zu liefern, die zur Risikominderung und Verbesserung der Reaktionszeiten beitragen.
- **Managed Extended Detection and Response (MXDR):** Geht über die Endpunkte hinaus und integriert Daten aus verschiedenen Quellen (Netzwerk, E-Mail, Cloud) für eine umfassendere Erkennung von Bedrohungen und deren Kontext.
- **Security Information and Event Management (SIEM):** Sammelt und analysiert Protokolle aus dem gesamten Unternehmen, um verdächtige Aktivitäten aufzudecken. Ideal für Compliance und Datenzentralisierung.
- **Ingestion:** Ein Auto ist ohne den richtigen Kraftstoff nutzlos. Dasselbe gilt für das SIEM. Es muss mit Protokollen aus Ihren vorhandenen IT-Ressourcen gefüttert werden - und die Menge der Protokolle, die Sie aufnehmen, wirkt sich auf die Kosten der Lösung aus. Wird in der Regel in Gigabyte pro Tag oder in Ereignissen pro Sekunde gemessen. (EPS).
- **Security Orchestration, Automation and Response (SOAR):** bezieht sich auf eine Reihe von Tools und Prozessen, die es Sicherheitsteams ermöglichen, Arbeitsabläufe für die Erkennung, Untersuchung und Reaktion auf Bedrohungen zu optimieren und zu automatisieren. Durch die Integration verschiedener Sicherheitssysteme und die Automatisierung sich wiederholender Aufgaben steigert SOAR die Effizienz, verkürzt die Reaktionszeiten und ermöglicht es den Analysten, sich auf höherwertige Aktivitäten zu konzentrieren.

## Menschen und Prozesse:

- **Managed Detection and Response (MDR):** Ausgelagerte Sicherheitsdienste, die Technologie (häufig SIEM oder XDR) mit einem Expertenteam für Erkennung, Untersuchung und Reaktion kombinieren.
- **Security Operations Centre (SOC):** Ein zentrales Team oder eine zentrale Einrichtung, das/die für die Überwachung und Reaktion auf Sicherheitsvorfälle zuständig ist, entweder intern oder von einem Anbieter verwaltet.

# Wie fügen sich diese zusammen?

Ein Managed Security Service besteht aus Menschen, Prozessen und Technologie. Die Technologie ist für die Erfassung aller für die Verwaltung des Dienstes erforderlichen Daten von entscheidender Bedeutung. Eine absolute Mindestanforderung ist ein EDR-Tool zur Bereitstellung von Daten über die Vorgänge an den Endpunkten. Viele Anbieter gehen über EDR hinaus zu XDR, das mehr als nur Endpunktdaten umfasst, um einen vollständigen Überblick über das gesamte Unternehmen zu erhalten.

XDR-Tools eignen sich hervorragend für die Erkennung von Vorfällen „in Echtzeit“, haben aber in der Regel einen eher kurzfristigen Blick auf die Welt. Viele Unternehmen entscheiden sich dafür, XDR durch eine SIEM-Lösung zu ergänzen, die rohe Protokolldaten über einen längeren Zeitraum speichert - in der Regel mindestens 90 Tage, aber auch mehrere Jahre. Zur Erfüllung der Compliance-Anforderungen Ihres Unternehmens kann der Einsatz eines SIEM-Systems erforderlich sein.

Die personellen und prozessualen Elemente werden in der Regel vom Managed Service Provider bereitgestellt. Wenn Sie bereits in die Technologie investiert haben, benötigen Sie einen Partner, der in dieser Technologie kompetent ist und Erfahrung, Regeln und Erkennungen auf der Grundlage dieses Anbieters aufgebaut hat, damit er sofort einen Mehrwert bieten kann. Wenn Sie noch nicht in diese Technologie investiert haben, werden Ihnen viele Partner gerne ein Angebot unterbreiten.

Wenn Sie sich für einen Partner im Bereich Managed Security entschieden haben, stellen Sie sicher, dass Sie auch das Ergebnis erhalten, das Sie gekauft haben. Wenn es sich bei der Technologie um einen etablierten Marktführer handelt, ist es wichtiger, einen Partner nach seinen Dienstleistungen und Fähigkeiten auszuwählen, als danach, wie gut er Ihre Sicherheitsanforderungen erfüllen kann. Konzentrieren Sie sich darauf, die Sicherheit gemeinsam zu verbessern, und überlassen Sie dem Partner die Technologie.

# SIEM vs. XDR: Worin besteht der Unterschied?

SIEM und XDR sind grundlegende Technologien für die Cybersicherheit. Sie dienen jedoch unterschiedlichen Zwecken:

| MERKMALE | SIEM | XDR |
|---|---|---|
| **Wichtigste Funktionen** | Sammelt und analysiert Protokolle, um die Einhaltung von Vorschriften zu gewährleisten und Bedrohungen zu erkennen. | Multimodale Bedrohungserkennung mit automatischer Reaktion. |
| **Bereitstellungsmodell** | Erfordert in der Regel interne Konfiguration und Wartung. | Wird als vollständiger Managed Service oder als Software-Plattform angeboten. |
| **Umfang** | Kundenspezifische Integrationen werden umfassend und flexibel unterstützt. | Engerer Anwendungsbereich, aber tiefere Integration zwischen den Support-Tools. |
| **Anwendungsfälle** | Am besten für Compliance-orientierte Unternehmen mit vorhandenem Fachwissen. | Ideal für Unternehmen, die eine vereinfachte und integrierte Erkennung und Reaktion wünschen. |

Beide haben ihre Stärken. Um alle Bereiche abzudecken, kombinieren viele Unternehmen die Compliance-Funktionen eines SIEM mit der erweiterten Bedrohungserkennung von XDR.

# Der geschäftliche Nutzen von Managed Security

Noch vor wenigen Jahrzehnten wurde in vielen Unternehmen überhaupt nicht über Sicherheit nachgedacht. Als die ersten Cyber-Bedrohungen auftauchten, begannen Unternehmen, in Virenschutz, Firewalls und andere grundlegende Sicherheitskontrollen zu investieren, um ihre Sicherheit zu gewährleisten. Der „Sicherheitsbeauftragte“ war für die Durchführung dieser Kontrollen zuständig, und die Dinge waren einfach. Mehr Bedrohungen bedeuteten auch mehr Kontrollinvestitionen. Die „Sicherheitskräfte“ werden zu einem Sicherheitsteam, in dem jedes Mitglied über unterschiedliche Fähigkeiten verfügt. Die Sicherung von Daten, Anwendungen, Infrastrukturen, Clouds und KI-Systemen erfordert unterschiedliche Fähigkeiten und diese müssen kohärent verwaltet werden, um eine durchgängige Sicherheitsabdeckung zu gewährleisten.

Die Kosten und die Komplexität des internen Sicherheitsmanagements bedeuten für viele ein  Einstiegshindernis. Die Alternative ist die Zusammenarbeit mit einem Managed Security Service Provider.

| ASPEKT | Internes SOC | MSSP-Partner |
|---|---|---|
| **Kosten** | Hohe Anschaffungskosten für Infrastruktur, Tools und Anpassungen. | Geringere Anschaffungskosten und laufende Kosten für Dienstleistungen durch die Bezahlung von Teilzeitkräften. |
| **Kompetenzen** | Erfordert die Einstellung und Bindung von hoch qualifizierten Fachkräften. | Zugang zu einem breiten Spektrum an Fachwissen ohne Personalbeschaffung. |
| **Skalierbarkeit** | Die Skalierung erfordert zusätzliche Investitionen in Ressourcen, Personal und Infrastruktur. | Einfach skalierbar mit bestehender Infrastruktur des MSSP. |
| **24/7-Abdeckung** | Mit eigenem Personal ist dies teuer und aufwendig. Für den Betrieb rund um die Uhr sind mindestens 12 Personen erforderlich. | In der Regel im Service enthalten. |

| ASPEKT | Internes SOC | MSSP-Partner |
|---|---|---|
| **Kontrolle** | Volle Kontrolle über SOC-Betrieb, Anpassungen und Priorisierung. | Begrenzte Kontrolle, mit einer gewissen Abhängigkeit von den Prozessen und der Priorisierung des MSSP. |
| **Implementierungszeit** | Längerer Zeitraum für die Einrichtung, Einstellung und Konfiguration. | Schnellere Einrichtung, da MSSPs oft über vorgefertigte Lösungen und Prozesse verfügen. |
| **Technologie-Updates** | Für die Aktualisierung der Tools und Technologien ist die Organisation verantwortlich. | MSSPs bieten im Rahmen des Dienstes Zugang zu den neuesten Tools und Technologien an. |
| **Compliance und Governance** | Gesamtverantwortung für die Einhaltung von Vorschriften und Bestimmungen. | MSSPs bieten in der Regel Dienstleistungen an, die den Compliance-Anforderungen entsprechen, aber nicht unbedingt unternehmensspezifische Nuancen abdecken. |
| **Threat Intelligence** | Erfordert den eigenständigen Aufbau oder das Abonnieren von Bedrohungsdaten-Feeds. | Zugang zu gesammelten Bedrohungsdaten von mehreren Kunden. |
| **Bedrohungsanalyse** | Hohe Anpassungsfähigkeit an organisationsspezifische Bedürfnisse und Arbeitsabläufe. | Standardisierte Angebote sind möglicherweise nicht vollständig auf individuelle Bedürfnisse zugeschnitten. |
| **Individuelle Anpassungen** | Ausgeprägtes Verständnis der Organisationsstruktur, der Prioritäten und des Kontextes. | Eingeschränktes Verständnis des spezifischen Unternehmenskontexts. |
| **Interne Zusammenarbeit** | Vereinfachte Koordination der SOC-Prozesse mit internen IT- und Sicherheitsteams. | Erfordert mehr Abstimmung zwischen dem Unternehmen und dem MSSP. |

# Wie hoch sind die Kosten für die Einrichtung eines internen Teams?

Die Einrichtung eines internen Security Operations Centers (SOC) erfordert eine sorgfältige finanzielle Planung, da mehrere Kostenfaktoren zu berücksichtigen sind:

### 1. Personalaufwand

- **SOC-Analysten:** Es ist von einem absoluten Minimum von zwei Analysten pro Schicht auszugehen, um unter Berücksichtigung von Krankheit, Urlaub und Burnout Prävention eine 24/7-Abdeckung zu gewährleisten.
- **Sicherheitsingenieure:** Für die Entwicklung, Verwaltung und Aktualisierung der SOC-Tools und -Infrastruktur sind mindestens zwei Ingenieure zuständig.
- **Spezialfunktionen:** Erwägen Sie, Incident Responders, Threat Hunters und einen SOC-Manager hinzuzuziehen, um die Effizienz des Teams zu gewährleisten.
- **Schulungen und Zertifizierungen:** Kontinuierliche Schulungen, um das Team über neue Bedrohungen, Tools und Compliance-Anforderungen auf dem Laufenden zu halten.

### 2. SIEM-Kosten (Sicherheitsinformations- und Ereignismanagement)

- **Lizenz- und Abonnementgebühren:** Die Kosten sind oft abhängig von der Protokolldatenmenge.
- **Infrastruktur:** Zusätzliche Kosten für Server, Speicher und Bandbreite können durch das Hosting des SIEM on premise oder in der Cloud entstehen.
- **Open-Source Alternativen:** Obwohl es kostenlose Plattformen gibt, können sie erhebliche Investitionen in qualifiziertes Personal oder externe Beratung für Einrichtung, Wartung und Abstimmung erfordern.

### 3. Kosten für Bedrohungsanalysen

- **Abonnements:** Bezahlter Zugriff auf Threat Intelligence Feeds zur Datenanreicherung und Kontextualisierung von Alerts.
- **Integration:** Zusätzliche Kosten für die Integration von Bedrohungsanalyse-Plattformen in Ihr bestehendes Ökosystem.

### 4. Kosten für Endgeräte-Erkennung und -Reaktion (EDR/XDR)

- **Tool-Lizenzen:** Lizenzen zur Erkennung und Reaktion von Bedrohungen auf Endgeräten und anderen Einrichtungen sowie in Netzwerken.
- **Skalierungskosten:** Kostenskala basierend auf der Anzahl der überwachten Geräte oder Assets.

### 5. Infrastrukturkosten

- **Hardware und Software:** Server, Speichergeräte und Software für die Protokollerfassung, Analyse und Speicherung.
- **Redundanz und Notfallwiederherstellung:** Sicherung von Systemen und Notfallwiederherstellungsplänen für den SOC-Betrieb.
- **Physischer Platzbedarf:** Sichere Büroräume oder ein spezieller Betriebsraum mit geeigneten Umweltkontrollen.

### 6. Überwachungs- und Erkennungsinstrumente

- Instrumente zur Überwachung von Netzwerkverkehr, Verhaltensanalysen und Einbruchsmeldesystemen (IDS/IPS).
- Regelmäßige Aktualisierungen und Anpassungen, um die Wirksamkeit gegen sich entwickelnde Bedrohungen zu gewährleisten.

### 7. Kosten für die Reaktion auf Vorfälle

- **Playbook-Entwicklung:** Zeit und Ressourcen zur Entwicklung detaillierter Prozesse und Arbeitsabläufe für die Reaktion auf Vorfälle.
- **Forensische Tools** Spezielle Tools für tiefgehende Untersuchungen von Verstößen oder verdächtigen Aktivitäten.

### 8. Kosten, um gesetzliche und regulatorische Anforderungen zu erfüllen

- Gewährleistung der Einhaltung von Industriestandards (z.B. ISO27001, NIS2, PCI DSS) können zusätzliche Investitionen in Tools, Prüfungen und Fachwissen erfordern.
- Überprüfung der Einhaltung von Vorschriften anhand regelmäßiger Bewertungen und Prüfungen.

### 9. Kosten für Schwachstellenmanagement

- Werkzeuge zum Scannen und Verwalten von Schwachstellen in Ihrer IT-Landschaft.
- Personal- oder Beratungszeit für Patch-Management und Korrekturmaßnahmen.

### 10. Lizenzierung für Sicherheitsplattformen

- Zusätzliche Lizenzkosten für DLP (Data Loss Prevention), Cloud-Sicherheitstools oder Firewalls, die in den Betrieb des SOC integriert sind.

### 11. Test-und Optimierungskosten

- **Penetrationstests:** Regelmäßiges Testen von SOC-Prozessen und Abwehrmechanismen zur Identifizierung von Lücken.
- **Übungen Rotes Team/Blaues Team:** Trainingsübungen zur Verbesserung der SOC-Bereitschaft und zur Verfeinerung der Fähigkeiten zur Reaktion auf Zwischenfälle.

### 12. Integration in bestehende IT-Systeme

- Kosten für die Integration von SOC-Tools in IT Managementsysteme wie Active Directory, Ticketing Systeme und ITSM-Plattformen.

### 13. Laufende Wartung und Updates

- Regelmäßige Software-Updates, Patches und Konfigurationsanpassungen.
- Austausch veralteter Hardware oder Software im Laufe der Zeit.

### 14. Beratungen und Partnerschaften mit Drittanbietern

- Kurzfristige Kosten für spezialisierte Berater zur Unterstützung bei der Ersteinrichtung oder komplexen Aufgaben.
- Potenzielle Partnerschaften mit Lieferanten für Support und Co-Management in frühen Betriebsphasen.

### 15. Versteckte und indirekte Kosten

- **Zeitaufwand:** Erheblicher Zeitaufwand für die Einrichtung, Feinabstimmung und Optimierung des SOC, bevor er vollständig betriebsbereit ist.
- **Opportunitätskosten:** Zeit und Ressourcen werden durch andere IT- und Sicherheitsprojekte abgelenkt.

# Was kostet die Zusammenarbeit mit einem MSSP?

Da der Anbieter bereits in alle oben genannten Posten investiert hat, zahlen Sie einen Teil dieser Kosten – in der Regel abhängig von Ihrem Verbrauch. Der Vorteil für Sie besteht darin, dass Sie nicht für ein ganzes Team zahlen müssen, das nicht voll ausgelastet ist, sondern Sie den Zugriff auf das Team haben, wenn Sie ihn benötigen.

Typische Anbieter von Managed Security Services setzen den Preis für eine Dienstleistung auf der Grundlage einer Kombination der folgenden Faktoren fest

- **Anzahl der Benutzer** – je mehr Nutzer, desto mehr Vorfälle sind zu bewältigen.
- **Anzahl der Endgeräte** – heutzutage haben Benutzer oft mehrere Endgeräte, und auch Server müssen überwacht werden.
- **Volumen der Protokolldaten** – Es gibt kleine Organisationen, die eine große Menge an Daten erzeugen, während es große Organisationen gibt, die möglicherweise über eine relativ einfache Infrastruktur verfügen. Anhand der Menge der von Ihnen generierten Protokolldaten können MSSPs den Umfang der erforderlichen Reaktion auf Vorfälle abschätzen.

Obwohl Sie wahrscheinlich die Anzahl der Benutzer und Endgeräte kennen – es sei denn, Sie verfügen bereits über ein SIEM oder SOC – ist das Volumen der Protokolldaten möglicherweise nicht bekannt. Ein guter Partner hilft Ihnen, diese Kosten auf der Grundlage der Anzahl und Art der Geräte, die Sie besitzen, abzuschätzen; diese Arbeit wird in der Regel im Rahmen des Vorverkaufs kostenlos durchgeführt.

Der Anbieter kann eine Vorauszahlung zur Deckung der Beratungskosten für die Einrichtung des Dienstes anbieten, gefolgt von einer monatlichen Gebühr, oder er kann beides in einer monatlichen Gebühr zusammenfassen. Idealerweise können sie mit beiden Möglichkeiten arbeiten, ganz nach Ihren Präferenzen.

Es können Kosten für die Lizenzierung der SIEM-Plattform anfallen. Dies kann in der monatlichen Gebühr enthalten sein oder separat an einen SaaS-Anbieter wie Microsoft oder Cisco gezahlt werden. Der Partner sollte deutlich darauf hinweisen, ob zusätzliche Gebühren an Dritte zu zahlen sind, und diese für Sie schätzen, um Ihnen einen Gesamtpreis zu nennen.

# SLAs & Berichterstattung: Die Grundlage des Service

Ein Service Level Agreement (SLA) definiert die Erwartungen, Verantwortlichkeiten und Leistungskennzahlen zwischen Ihnen und Ihrem Managed Security Anbieter. Ein starkes SLA sorgt für Klarheit, Rechenschaftspflicht und Anpassung an die Anforderungen Ihres Unternehmens – jedoch sind nicht alle SLAs gleich.

- **Mittlere Zeit bis zur Erkennung:** Wie viel Zeit vergeht zwischen dem Auftreten eines Vorfalls und seiner Entdeckung durch das SOC? Bei modernen SIEM-Plattformen sollte die Erkennung nahezu in Echtzeit erfolgen – die Erkennung eines Vorfalls hängt jedoch davon ab, wie gut die Plattform konfiguriert ist, welche Protokollquellen aufgenommen werden und die Qualität der Regeln. Es ist schwierig, SLAs auf dieser Ebene direkt zu vergleichen.
- **Mittlere Reaktionszeit:** Wie schnell reagiert der SOC, sobald ein Vorfall erkannt wird? Obwohl dies oft die wichtigste Maßnahme ist, ist es nicht einfach, den Partner zu finden, der am schnellsten ist... (siehe Info “Wie sieht ein gutes SLA aus?”)
- **Mittlere Behebungszeit:** Wie lange dauert es von der Antwort bis zur Lösung des Problems? Es gibt eine große Bandbreite an Arten und Komplexitäten von Vorfällen, so dass auch diese Zahl nur schwer vergleichbar ist. Darüber hinaus kann es vorkommen, dass einige Abhilfemaßnahmen nur von Ihrem internen IT-Team oder einem Dritten durchgeführt werden können - MSSPs schließen diese Zeiten von diesem SLA aus.

# Wie ein gutes SLA aussieht

Ein gut durchdachtes SLA schafft ein Gleichgewicht zwischen Leistung und Zweckmäßigkeit. Suchen Sie:

- **Risikobasierte Priorisierung:** Höhere Dringlichkeit für kritische Vorfälle und geringere Priorität für kleinere Probleme.
- **Transparente Metriken:** Klare Definitionen von Reaktions- und Lösungszeiten mit messbaren Ergebnissen.
- **Realistische Zeitpläne:** Oberflächlich betrachtet mag eine Reaktionszeit von 5 Minuten besser erscheinen als eine Reaktionszeit von 30 Minuten. Aber was ist der Inhalt einer „Antwort“? Wollen Sie wirklich jede Nacht um 3 Uhr angerufen werden, weil ein Partner sein SLA über die Beseitigung von Fehlalarmen stellt? Sie bezahlen den Partner dafür, dass er wirklich positive Meldungen auswertet und bestätigt - und nicht einfach jede Meldung vom SIEM direkt an Sie weiterleitet.

SLAs sind die Grundlage des Vertrauens zwischen Ihnen und Ihrem Anbieter. Ein gutes SLA garantiert nicht nur Schnelligkeit, sondern auch Qualität, Verantwortlichkeit und Übereinstimmung mit Ihren Geschäftszielen.

# Berichtswesen

In der Regel gibt es zwei Arten von Berichten. “Ad-hoc-Berichte, die erstellt werden, wenn ein Vorfall entdeckt und Ihnen gemeldet wird. Sie dienen dazu, schnell auf ein Problem aufmerksam zu machen - in der Regel auf ein Problem, das Ihr Eingreifen oder eine rechtzeitige Benachrichtigung erfordert.

Der MSSP sollte jedoch nicht nur bei Problemen eingreifen. Es sollten regelmäßige Treffen mit technischen und wirtschaftlichen Interessenvertretern stattfinden, bei denen Themen wie diese behandelt werden:

- **Abdeckung der Protokollquellen:** Der Service ist nur so gut wie die Protokolle, auf die er Zugriff hat. Verwendet der Anbieter ein Framework wie z. B. MITRE ATT&CK, um Sie auf zusätzliche Quellen für Protokolle aufmerksam zu machen, die einen Mehrwert darstellen könnten?
- **Leistung im Vgl. zum SLA:** Dies ist eine Gelegenheit, die Leistung des Dienstes im Vergleich zu den SLAs zu überprüfen. Bei Bedarf können Korrekturpläne erstellt werden.
- **Überprüfung früherer Vorfälle:** Rückblick auf einige schwerwiegendere Vorfälle - was ist gut gelaufen, was könnte verbessert werden?
- **Ein Blick über den Tellerrand:** Die Welt steht nicht still – Ihr Unternehmen wird sich im Laufe der Zeit ebenso verändern wie die Bedrohungslandschaft. Sie sollten die Möglichkeit haben, den Anbieter regelmäßig über alle geschäftlichen Veränderungen (z. B. Fusionen und Übernahmen) zu informieren, die sich auf den Dienst auswirken könnten, und der Anbieter sollte Einblicke in neue Bedrohungen und Lösungen geben können.

# Fähigkeiten, auf die Sie bei einem Managed Security Partner achten sollten

## Automatisierung & KI

Moderne Bedrohungen erfordern eine schnelle Erkennung und Reaktion. Anbieter sollten Automatisierung und KI nutzen, um:

- Anomalien in Echtzeit zu erkennen,wodurch die Abhängigkeit von manuellen Analysen verringert wird.
- Arbeitsabläufe bei der Reaktion auf Vorfälle zu optimieren und eine schnelle Eindämmung zu gewährleisten.
- Gängige Aktionen, wie die Isolierung eines Geräts oder die Sperrung eines kompromittierten Kontos zu automatisieren. Dies ist besonders wichtig, wenn der Partner auch außerhalb der Geschäftszeiten für Sie tätig werden soll.

## Bedrohungsanalyse

Umfassende Bedrohungsinformationen helfen, den sich entwickelnden Risiken einen Schritt voraus zu sein. Suchen Sie nach Anbietern, die:

- Bedrohungsdaten aktuell halten und integrieren sie diese in ihre Dienste.
- Einblicke in neue Angriffstrends gewähren, die für Ihre Branche relevant sind.
- Informationen zur besseren Erkennung und Priorisierung kritischer Bedrohungen nutzen.

## Jagd auf Bedrohungen

Proaktive Bedrohungserkennung stellt sicher, dass Bedrohungen nicht unentdeckt bleiben. Bewerten Sie, ob der Anbieter:

- Regelmäßige manuelle Aktivitäten zur Gefahrenabwehr anbietet.
- Fortschrittliche Instrumente zur Erkennung versteckter Risiken einsetzt.
- Detaillierte Berichte über die Ergebnisse und Abhilfemaßnahmen erstellt.

## Wiederherstellung

Warnungen sind nur ein Teil der Gleichung – wirksame Abhilfemaßnahmen sind entscheidend. Stellen Sie sicher, dass der Anbieter:

- Klare Anleitungen zu Eindämmungsstrategien bietet.
- Über Beratungskapazitäten verfügt, um Sie bei der Durchführung größerer Projekte zur Verbesserung der Sicherheitsreife zu unterstützen.

# Praktische Überlegungen

## Akkreditierungen

Jeder Partner kann Ihnen ausgefeiltes Marketingmaterial vorlegen, aber welche externe Validierung kann er für die Effektivität seines Angebots liefern?

- Achten Sie auf eine unvoreingenommene externe Validierung durch Quellen wie MSSP Alert: www.msspalert.com/top-250

- Prüfen Sie, ob Sie beim Anbieter Ihrer Wahl akkreditiert sind. Vergewissern Sie sich, dass der Anbieter Experte für die von ihnen verwendeten Tools ist und dass ihr Service durch den Anbieter geprüft wird. Dies ist auch ein Hinweis darauf, dass sie im Hinblick auf Verbesserungen eng mit dem Lieferanten zusammenarbeiten und gute Beziehungen zu dessen Entwicklungsteam haben.

- Überprüfen Sie, ob relevante Compliance-Rahmenwerke vorhanden sind, die in Ihrer Region oder Branche relevant sind. Zertifikate wie Cyber Essentials+ und ISO27001 zeigen, dass das Unternehmen seine eigene Sicherheit ernst nimmt, und sollten eine Mindestanforderung für einen Sicherheitsanbieter sein.

# Onboarding-Prozess

Von einem guten Partner können Sie erwarten, dass er Sie durch den Einführungsprozess führt. In der folgenden Tabelle sind die wichtigsten Schritte aufgeführt. Auch wenn der Partner die Hauptarbeit leisten sollte, ist es wichtig, dass Sie sich über mögliche Abhängigkeiten Ihrer Mitarbeiter im Klaren sind, damit Sie diese einplanen können.

| Was | Ihre Beteiligung |
|---|---|
| **Scoping und Discovery:** Um eine geeignete Lösung anbieten zu können, muss der Partner viele Fragen zu Ihren Erwartungen an den Dienst und zu Ihrer derzeitigen technischen Ausstattung stellen. | Sie sollten davon ausgehen, dass Sie mehrere Beteiligte einbeziehen müssen, um einen Überblick über die Zusammensetzung und den Umfang Ihres Unternehmens zu erhalten. Wenn Sie z. B. die Anzahl der Endgeräte, die Marke, das Modell und die Anzahl der Firewalls, Cloud-Dienste und anderen Ressourcen kennen, können Sie sicherstellen, dass das Design Ihren Anforderungen entspricht. |
| **Plattform-Aufbau:** Wenn ein SIEM-Tool eingesetzt oder XDR in Ihrem Unternehmen eingeführt werden soll, müssen Sie einbezogen werden, um sicherzustellen, dass die Benutzer so wenig wie möglich gestört werden. | Um das SIEM einzurichten, muss Ihr IT-Team dem Partner möglicherweise Zugriff auf Ihre Cloud-Umgebung gewähren. Sie sollten in Zusammenarbeit mit dem Partner einen gemeinsamen Plan erstellen, wie und wann die Endpunkt-Agenten eingesetzt werden sollen. |
| **Individuelle Anpassungen:** Jeder gute Partner verfügt über eine Reihe von Standardregeln, die in den meisten Unternehmen verwendet werden, um Vorfälle zu erkennen. Wenn Sie jedoch spezielle Anpassungen benötigen, müssen Sie mit dem Partner zusammenarbeiten, um sicherzustellen, dass diese Anforderungen berücksichtigt werden. | Wenn Sie bestehende Regeln in einem Altsystem haben, die umgeschrieben werden müssen, kann die Bereitstellung dieser Regeln zu einer schnelleren Einführung führen, als wenn Sie bei Null anfangen würden. Wenn es sich um neue Anforderungen handelt, kann die Dokumentation dieser Anforderungen in natürlicher Sprache helfen, dem Partner Ihre Bedürfnisse zu vermitteln. |
| **Frühzeitige Unterstützung:** Nach Inbetriebnahme des Dienstes ist eine weitere Optimierungsphase erforderlich, um Fehlalarme zu reduzieren und das System an Ihre spezifische Umgebung anzupassen. | Eine enge Zusammenarbeit zwischen Ihrem IT-Team und dem Partner ist gefragt. Viele Vorfälle können vom Partner leicht als falsch oder richtig eingestuft werden. Er wird in der “Grauzone” zusammenarbeiten wollen, um Regeln anzupassen und Artikel für die Wissensdatenbank zu schreiben. So können falsch-positive Vorfälle minimiert werden. |
| **Live-Betrieb:** Nach Abschluss der ersten Phase der Lebenserhaltung ist die Lösung in einem stabilen Zustand. Die Anpassungsarbeit des Partners hört hier nicht auf, sollte sich aber deutlich verlangsamen, wenn der Schwerpunkt auf die Erkennung von Vorfällen verlagert wird. | Erstellen Sie eine Liste mit Kontaktpersonen, die im Falle eines Sicherheitsvorfalles benachrichtigt werden müssen. Für kleinere Unternehmen könnte dies eine Verteilerliste sein, die auch komplexere Aspekte wie unterschiedliche Eskalationspfade oder spezielle Gruppen von Problemlösern für bestimmte Technologien enthalten könnte. Dazu können auch Dritte gehören, wenn Sie bestimmte Tätigkeiten ausgelagert haben. |

# Value-added Services

Auch wenn Ihr Hauptanliegen bei der Suche nach einem Anbieter von Managed Security Services darin besteht, Ihnen bei der Erkennung und Behebung von Sicherheitsvorfällen zu helfen, gibt es oft noch andere Dienstleistungen, die ganz natürlich zu einem Managed Security Services-Anbieter gehören. Oft ist es von Vorteil, wenn mehrere Dienstleistungen von ein und demselben Partner erbracht werden, da dieser einen besseren Überblick über Ihre Sicherheit hat und oft fundiertere Entscheidungen treffen kann.

Das **Schwachstellenmanagement** ist eine natürliche Ergänzung zu einem SOC, da es proaktiv Sicherheitslücken in der digitalen Umgebung eines Unternehmens identifiziert, bewertet und priorisiert. Durch die Integration dieses Dienstes profitieren Unternehmen von einer kontinuierlichen Überwachung und umsetzbaren Plänen zur Behebung von Schwachstellen, die auf die SOC-Fähigkeiten zur Bedrohungserkennung abgestimmt sind. Dadurch wird das Risiko eines Missbrauchs verringert, da Sicherheitslücken geschlossen werden, bevor sie von Angreifern ausgenutzt werden können.

**Digital Risk Protection Services (DRPS)** sind eine weitere strategische Ergänzung, die die Reichweite des SOC über das Unternehmensnetzwerk hinaus auf die digitale Landschaft ausweitet. DRPS überwacht Bedrohungen in externen Umgebungen wie dem Dark Web, sozialen Medien und externen Systemen. Durch die Identifizierung von Markenidentitäten, Zugangsdatenlecks oder offen gelegten sensiblen Daten können Unternehmen frühzeitig vor potenziellen Bedrohungen gewarnt werden, so dass das SOC schnell reagieren und Risiken minimieren kann.

Für Unternehmen, die mit aktiven Bedrohungen oder Sicherheitsverletzungen konfrontiert sind, gewährleistet die Kombination von **Digital Forensics and Incident Response (DFIR)** mit Managed Security eine schnelle Eindämmung und detaillierte Analyse nach dem Vorfall. DFIR-Teams können die Telemetrie und die Protokolle des SOC nutzen, um die Ursachen zu untersuchen, das Ausmaß der Sicherheitsverletzung zu bestimmen und Wiederherstellungsmaßnahmen zu empfehlen. Dieser ganzheitliche Ansatz ermöglicht es den Unternehmen, entschlossen zu reagieren und gleichzeitig Erkenntnisse zu gewinnen, um eine Wiederholung zu vermeiden. Durch die Bündelung dieser Dienste entsteht eine nahtlose End-to-End-Sicherheitslösung, die Unternehmen Vertrauen in Prävention und Widerstandsfähigkeit gibt.

# Nächste Schritte

Die Bedrohungen der Cybersicherheit nehmen zu, und die Kosten der Untätigkeit sind hoch. Kontaktieren Sie Insight, einen führenden MSSP, und erfahren Sie, wie Sie Ihr Unternehmen mit unseren Managed Security Services kostengünstig schützen können.

**at.insight.com**
**ch.insight.com**
**de.insight.com**

**+43 720 700 285**
**+41 44 878 7606**
**+49 6134 288 288**

[1] source: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

[2] source: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

[3] source: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report