N-ABLE™ INFINIGATE

Argumente für Managed-SOC-Dienstleistungen

Kurzleitfaden für die Renditeberechnung

eGuide

Argumente für Managed-SOC-Dienstleistungen:
Kurzleitfaden für die Renditeberechnung

Cyberbedrohungen werden zunehmend raffinierter, somit steigt auch der Bedarf an qualifizierten Cybersecurity-Experten. Die jüngste 2022 (ISC)² Cybersecurity Workforce Study[1] hat gezeigt, dass die Personallücke im Bereich der Cybersicherheit im vergangenen Jahr mehr als doppelt so stark gewachsen ist wie die Zahl der eingestellten Mitarbeiter, und zwar mit einem Anstieg von 26,2 % im Vergleich zum Vorjahr. 70 % der Befragten waren der Meinung, dass ihre Unternehmen nicht genügend Mitarbeiter für die Cybersicherheit haben, und mehr als 50 % waren der Meinung, dass der Personalmangel das Unternehmen einem Risiko für Cyberangriffe aussetzt.

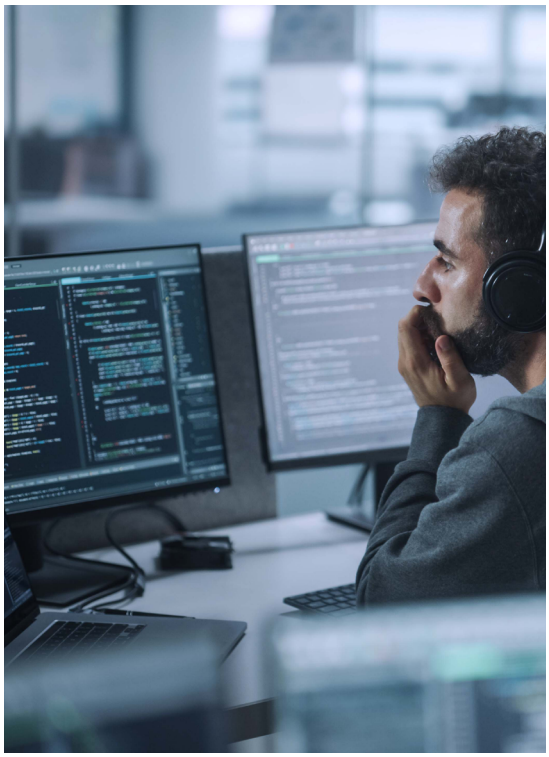
Vor diesem Hintergrund verlassen sich zunehmend mehr Unternehmen auf MSPs, um ihre IT-Sicherheit im Alltag zu verwalten. Aber auch die MSPs stehen vor der gleichen Herausforderung. Wenn IT-Techniker die Überwachung von Sicherheitsvorgängen für eine größere Anzahl von Kunden übernehmen, kann ihre Alarmmüdigkeit zunehmen und die tägliche Arbeitsbelastung ansteigen. Und eine Entlastung der IT durch die Einstellung von zusätzlichem Personal wird durch den vorherrschenden Arbeitskräftemangel im Sicherheitsbereich erschwert. Selbst MSPs, die ein eigenes Sicherheitscenter (Security Operations Center, kurz SOC) betreiben, stehen bei der Ausweitung ihrer Sicherheitsdienstleistungen vor den gleichen Herausforderungen.

Wie also können MSPs diese Herausforderungen meistern? Eine Partnerschaft mit einem Managed-SOC-Anbieter kann die ideale Lösung sein, unabhängig davon, ob der MSP bereits über ein SOC verfügt oder nicht.

Warum Managed SOC?

Ein Managed SOC ist eine verwaltete Sicherheitsdienstleistung, die es Unternehmen ermöglicht, die Erkennung von Gefahren und die Reaktion auf Zwischenfälle an ein externes SOC auszulagern. Mit diesem Angebot in Form eines Abonnements können Unternehmen auf ein Team von Cybersecurity-Experten zugreifen, die als Erweiterung ihrer IT-Teams fungieren und die operativen Aufgaben der Überwachung der gesamten Infrastruktur rund um die Uhr übernehmen – also die Identifizierung und Untersuchung von Bedrohungen und die Reaktion darauf.

Ein Managed SOC kann Ihnen dabei helfen, die bestehenden Kosten zu senken und Ihr Sicherheitsangebot zu erweitern, um mehr Einnahmen zu erzielen, während Sie gleichzeitig mehr Kunden betreuen, ohne zusätzliches Personal einzustellen. Mit anderen Worten: Ein Managed SOC kann Ihnen helfen, Ihr Unternehmen zu skalieren, indem Sie zeitaufwändige Aufgaben an einen erfahrenen Cybersecurity-Partner übertragen.



[1]https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

Kurzleitfaden für die Renditeberechnung

Diese Vorteile können durch eine einfache Renditeberechnung nachgewiesen werden. Hier finden Sie einen kurzen Leitfaden zur Rendite sowie Beispiele, die die folgenden Aspekte berücksichtigen:

1. Betriebskosten für Sicherheitscenter
2. Kosteneinsparungen mit einem Managed SOC
3. Umsatzsteigerung durch die Zusammenarbeit mit einem Managed SOC

1. Betriebskosten für Sicherheitscenter

Um besser zu verstehen, wie eine Managed-SOC-Dienstleistung Ihnen helfen kann, Ihre Kosten zu senken, müssen Sie über die Lizenzkosten Ihrer Schutzlösung für Endpunkte hinausblicken. Eine genauere Bewertung der Kosten berücksichtigt auch die Zeit, die für das Monitoring, die Reaktion auf einen Vorfall und dessen Behebung und nicht zuletzt für die Planung der Schadensbegrenzung aufgewendet wird, sowie die Zeit für die Bedrohungserkennung, die Gehälter inkl. Lohnnebenkosten[2] für Vollzeitmitarbeiter (VZÄ) sowie die Notwendigkeit, ein SOC 24x7x365 zu besetzen.

Wenn es sich bei der von Ihnen verwendeten Endpunkt-Schutzlösung um eine Antivirenlösung (AV) handelt, wären diese Kosten wahrscheinlich noch höher als bei einer EDR (Endpoint Detection and Response)-Lösung. Im Gegensatz zu EDR verfügt AV nicht über automatische Abhilfemaßnahmen oder detaillierte Forensik. Das bedeutet, dass Techniker ein Bedrohungsereignis untersuchen, die Grundursache identifizieren, den entstandenen Schaden beheben und weitere Anzeichen für eine Kompromittierung untersuchen müssen – und alles manuell und ohne hochwertige Telemetrie- und Analysedaten. Dieser gesamte Prozess kann mit AV sogar 3x länger dauern als mit EDR[3], was die mit der AV-Lösung verbundenen Kosten in die Höhe treibt. Ganz zu schweigen davon, dass eine proaktive Bedrohungserkennung mit AV gar nicht möglich ist und eine Untersuchung nach der Infektion aufgrund fehlender forensischer Informationen fast nie durchgeführt wird.

Wenn Sie fortschrittlichere Sicherheitsverfahren nutzen und ein eigenes SOC betreiben, müssen Sie auch die Personalkosten für das SOC berücksichtigen.

Ein SOC-Team besteht in der Regel aus Sicherheitsanalysten, die Bedrohungsvorfälle untersuchen, darauf reagieren und die Einhaltung von Branchenvorschriften sicherstellen (Tier-1- und 2-Analysten), sowie aus Cybersecurity-Leitern, die Tätigkeiten zur Bedrohungserkennung durchführen, um proaktiv nach Bedrohungen zu suchen, die möglicherweise andere Verteidigungsmaßnahmen umgangen haben, diese einzudämmen und sich um Eskalationen zu kümmern (Tier-3-Analysten). Eine genaue Bewertung der mit einem SOC verbundenen Personalkosten berücksichtigt nicht nur die VZÄ-Gehälter der Analysten, sondern auch die Lohnnebenkosten. Um ein besseres Verständnis dafür zu bekommen, wie die SOC-Personalkosten aussehen könnten, können wir uns verfügbare Branchendaten ansehen und einige Schätzungen anstellen.

Die Renditebeispiele und bewährten Verfahren in diesem Leitfaden wurden von Lewis Pope, dem Security HeadNerd von N-able, für Sie zusammengestellt.

Folgen Sie dem N-able Head-Nerds-Team für Informationen zu bewährten Verfahren, Sicherheitsveranstaltungen und Bootcamps, mit denen Sie Ihr MSP-Business ausbauen können.

[2]https://www.accountingtools.com/articles/what-is-a-burden-rate.html
[3]https://www.n-able.com/de/blog/edr-vs-antivirus-three-reasons-to-step-up-your-game

Hier ist ein Beispiel – Hypothetisches Szenario:

- Tier 1 SOC-Analyst Gehaltsspanne $40K-$81K I **Mittelwert $60,5K**[4]
- Tier 2 SOC-Analyst Gehaltsspanne $48K-$116K I **Mittelwert $82k**[5]
- Tier 3 SOC-Analyst/Senior Leitender Analyst für Cybersicherheit $83K-$206K I **Mittelwert $144,5K**[6]
- VZÄ-Kostenmultiplikator / Belastungssatz pro Arbeitskraft = **1,25**[7]
- 24x7x365 Personalbesetzung für 1 Tier 1, alle Schichten = 8760 Arbeitsstunden
- 24x7x365 Personalbesetzung für 1 Tier 2, alle Schichten = 8760 Arbeitsstunden
- 1 Tier 3 Senior Leitender Analyst für Cybersicherheit/Threat Hunter für eine Schicht pro Tag = 2080 Arbeitsstunden

Wenn wir von diesem Szenario ausgehen, ergeben sich die folgenden geschätzten Kosten:

- Mittleres Tier 1 SOC-Analysten-Gehalt = $65.500,00
  - Mittleres Tier 1 SOC-Analysten-Gehalt pro Stunde = Mittleres Tier 1 SOC-Analysten-Gehalt x VZÄ-Kostenmultiplikator = $60.500,00/2080 x 1,25 = $36,36
- Mittleres Tier 2 SOC-Analysten-Gehalt = $82.000,00
  - Mittleres Tier 2 SOC-Analysten-Gehalt pro Stunde = Mittleres Tier 2 SOC-Analysten-Gehalt x VZÄ-Kostenmultiplikator = $82.000,00/2080 x 1,25 = $49,28
- Mittleres Gehalt Senior Leitender Analyst für Cybersicherheit/Threat Hunter = $144.500,00
  - Mittleres Gehalt Senior Leitender Analyst für Cybersicherheit/Threat Hunter pro Stunde = $144.500,00/2080 x 1,25 = $86,84
- **Gesamtsumme Gehälter inkl. Lohnnebenkosten pro Monat** = (Mittleres SOC-Analysten-Gehalt Tier 1 pro Stunde x 8760) + (Mittleres SOC-Analysten-Gehalt Tier 2 pro Stunde x Arbeitsstunden) + (Mittleres Gehalt Senior Leitender Analyst für Cybersicherheit pro Stunde x Arbeitsstunden) / 12 Monate = ($36,36 x 8760 + $49,28 x 8760 + $86,84 x 2080) / 12 Monate = **$77.569,47**
- **Gesamtsumme Gehälter inkl. Lohnnebenkosten pro Jahr** = (Mittleres SOC-Analysten-Gehalt Tier 1 pro Stunde x 8760) + (Mittleres SOC-Analysten-Gehalt Tier 2 pro Stunde x Arbeitsstunden) + (Mittleres Gehalt Senior Leitender Analyst für Cybersicherheit pro Stunde x Arbeitsstunden) = $36,36 x 8760 + $49,28 x 8760 + $86,84 x 2080 = **$930.833,60**

[4]https://www.glassdoor.com/Search/results.htm?keyword=tier%201%20soc%20analyst (Zugriff Dezember 2022)
[5]https://www.glassdoor.com/Search/results.htm?keyword=tier%202%20soc%20analyst (Zugriff Dezember 2022)
[6]https://www.glassdoor.com/Career/principal-cybersecurity-analyst-career_KO0,31.htm (Zugriff Dezember 2022)
[7]https://www.accountingtools.com/articles/what-is-a-burden-rate.html

2. Kosteneinsparungen mit einem Managed SOC

Wenn Sie noch kein eigenes SOC eingerichtet haben, wird es in Zukunft wahrscheinlich noch schwieriger sein, dies zu tun. Und wenn Sie sich die geschätzten Kosten für SOC-Personal ansehen, lohnt es sich dann überhaupt, den Aufwand zu betreiben, wenn es einfachere und schnellere Alternativen gibt, um Ihre Wachstumsziele zu erreichen?

Ein Managed-SOC-Anbieter kann Ihnen helfen, die für die Einrichtung eines SOC anfallenden Kosten in strategischere Initiativen umzuleiten. Gleichzeitig können Sie die Zeit, die Ihr Team mit dem Monitoring und der Lösung von Bedrohungsvorfällen verbringt, verringern, wodurch sich wiederum Personalkosten einsparen lassen.

Nehmen wir Folgendes an:

- Mittlere Zeit bis zur Entdeckung (pro Bedrohungsfall) = 0,15 Stunden
- Mittlere Reaktionszeit (pro Bedrohungsfall) = 0,50 Stunden
- Mittlere Zeit bis zur Behebung (pro Bedrohungsfall) = 0,50 Stunden
- Durchschnittliche Anzahl von Bedrohungsereignissen pro Monat = 40
- VZÄ-Gehalt für Techniker/Ingenieure = $45.000
- VZÄ-Kostenmultiplikator / Belastungssatz pro Arbeitskraft = 1,25
- 2080 Arbeitsstunden pro Jahr

Das bedeutet:

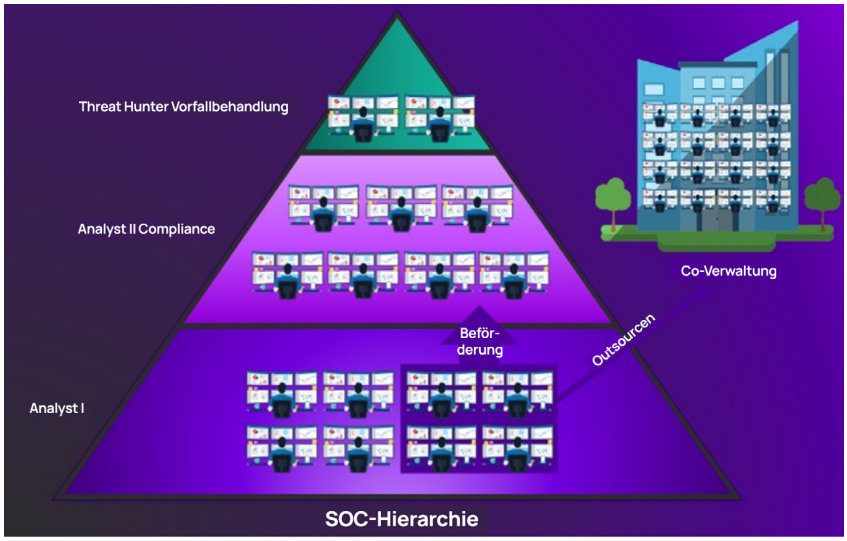
- Mittlere Gesamtzeit zur Lösung eines Bedrohungsvorfalls/Arbeitsstunden pro Bedrohungsvorfall = 0,15 + 0,50 + 0,50 = 1,15 Stunden
- Arbeitsstunden pro Monat = 40x1,15 = 46
- Arbeitsstunden pro Jahr = 40x1,15x12 = 552
- VZÄ Kosten für Techniker/Ingenieure pro Stunde = ($45.000/2080) x 1,25 = $27,04
- Personalkosten pro Bedrohungsfall = Arbeitsstunden pro Bedrohungsfall x VZÄ-Kosten für Techniker/Ingenieure pro Stunde = 1,15 x $27,04 = $31,10

Indem Sie die Arbeit, die mit der Lösung eines Bedrohungsvorfalls verbunden ist, auslagern, könnten Sie, basierend auf den obigen Annahmen und vorläufigen Berechnungen, die folgenden Einsparungen bei den Arbeitsstunden und Personalkosten erzielen:

- Eingesparte Arbeitsstunden pro Bedrohung = Arbeitsstunden pro Bedrohungsfall = 1,15
- Eingesparte Arbeitsstunden pro Monat = Arbeitsstunden pro Monat = 46
- **Eingesparte Arbeitsstunden pro Jahr = Arbeitsstunden pro Jahr = 552**
- Eingesparte Personalkosten pro Bedrohungsfall = Arbeitsstunden pro Bedrohungsfall x Personalkosten pro Bedrohungsfall = 1,15 x $31,10 = $35,76
- Einsparungen bei den Personalkosten pro Monat = Durchschnittliche Anzahl von Bedrohungsereignissen pro Monat x eingesparte Personalkosten pro Bedrohungsereignis = 40 x $35,76 = $1.430,59
- **Eingesparte Personalkosten pro Jahr = Eingesparte Personalkosten pro Monat x 12 (Monate) = $1.430,59 x 12 = $17.167,07**

Wenn Sie ein SOC besitzen, können Sie ebenfalls Arbeitsstunden und Personalkosten einsparen. Indem Sie einen Teil Ihrer SOC-Aktivitäten an einen Managed-SOC-Partner auslagern, können Sie Ihre Mitarbeiter zumindest teilweise entlasten und ihnen die Möglichkeit geben, in ihrer derzeitigen Rolle zu wachsen oder zusätzliche Aufgaben zu übernehmen.

Wenn Sie andererseits nicht mit einem Managed SOC zusammenarbeiten, das Ihnen bei der Mitbetreuung Ihrer Aufgaben hilft, entstehen Ihnen Opportunitätskosten. Dabei werden die Arbeitsstunden berücksichtigt, die erforderlich sind, um Mitarbeiter für das 24x7x365-Monitoring, die Sichtung und die Beseitigung von erkannten Bedrohungen bereitzuhalten.



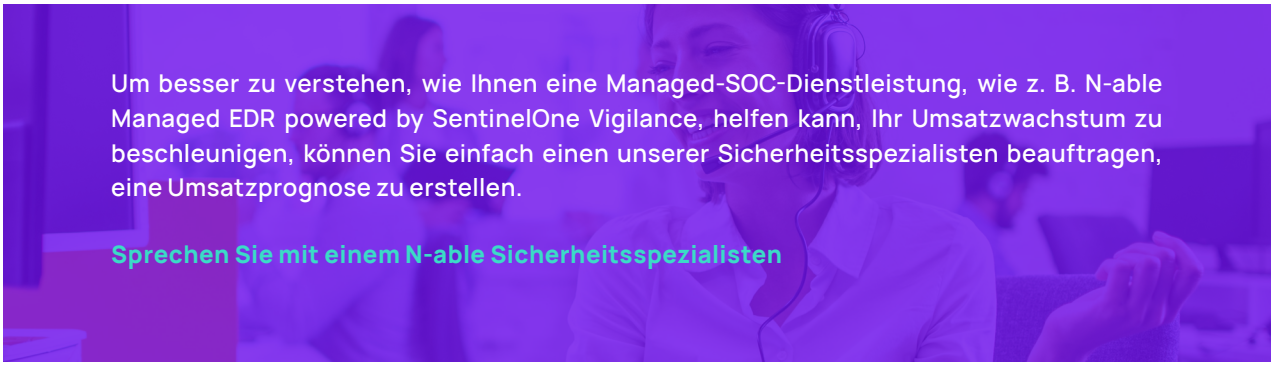
Sie können es so betrachten:

Wenn Sie Ihr Geschäft ausbauen wollen, indem Sie weitere Kundeneinsätze hinzufügen, werden Sie dann in der Lage sein, eine 24x7x365-Betreuung für alle Projekte zu gewährleisten, insbesondere angesichts des Fachkräftemangels im Bereich der Cybersicherheit?

3. Umsatzsteigerung durch die Zusammenarbeit mit einem Managed SOC

Die Partnerschaft mit einem Managed-SOC-Anbieter bietet mehr als nur die Möglichkeit, die Kosten für die Einrichtung eines SOC oder die Übernahme zusätzlicher Aufgaben umzuleiten. Sie ermöglicht es MSPs, die kein eigenes SOC besitzen, ihr Angebot um fortschrittliche Sicherheitsdienstleistungen zu erweitern und neue Einnahmequellen zu erschließen, und zwar mit beträchtlichen Gewinnspannen – denn Arbeitskräfte und Fachwissen im Bereich der Cybersicherheit sind heutzutage wirklich knapp.

Und selbst MSPs, die bereits ein SOC besitzen, können ein Managed SOC nutzen, um ihr eigenes zu ergänzen. Sie können mehr Kunden mit unterschiedlichem Projektaufwand übernehmen, da sie wissen, dass sie Personal und Fachwissen im Bereich Cybersicherheit garantieren können, wodurch sie Größenvorteile erzielen und ihr Umsatzwachstum beschleunigen können.



Weitere Überlegungen

Der Fachkräftemangel im Bereich der Cybersicherheit ist inzwischen eine globale Realität, mit mehr als 700.000 offenen Stellen (Stand Januar 2023)[8] alleine in den USA. In diesem Klima müssen MSPs ihren Personalbedarf überdenken, Wege finden, um die Lücken zu schließen, und sich der Herausforderung stellen, erfahrene Mitarbeiter einzustellen, um eine 24x7x365-Dienstleistung zu gewährleisten.

Wenn Sie sich die aktuellen Trends im Bereich der Cybersecurity-Versicherung ansehen, müssen Sie möglicherweise bald erwägen, Ihre Tätigkeit um fortschrittliche Sicherheitsdienstleistungen zu erweitern, da sich die Anforderungen in Sachen Cybersecurity-Versicherung rasant weiterentwickeln. Einige Ihrer Kunden gelten möglicherweise als Hochrisikokunden, was Ihr Risikoprofil erhöht und sich auf Ihre Cyberversicherungsprämie auswirkt, während andere Kunden zusätzliche erweiterte Dienstleistungen benötigen, um die Sicherheitsanforderungen für ihre eigene Cyberversicherungspolice zu erfüllen.

Möglicherweise kommen Sie in die Lage, dass Sie die Cybersicherheit für einige Ihrer Kunden mitverwalten sollen, die beispielsweise einen weiteren Sicherheitsanbieter für SOC-Dienstleistungen beauftragen möchten. Wenn Sie in solchen Fällen bereits mit einem Managed-SOC-Anbieter zusammenarbeiten, können Sie die Anforderungen dieser Kunden erfüllen, ohne dass diese einen Dritten beauftragen müssen. Auf diese Weise erhalten Sie eine bessere Kontrolle über deren Cybersicherheit und können mögliche Sicherheitslücken vermeiden. Der Schlüssel dazu ist, sich als Cybersecurity-Experte Ihrer Kunden zu positionieren. Dabei geht es nicht nur darum, deren aktuelle Bedürfnisse zu erfüllen, sondern auch darum, die Mittel zu haben, um ihre zukünftigen Anforderungen zu erfüllen und sie auf ihre Optionen und Möglichkeiten aufmerksam zu machen.

Ein Managed-SOC-Dienst wie N-able Managed EDR powered by SentinelOne Vigilance verschafft Ihnen den dringend benötigten Zugang zu einem Team renommierter Cybersecurity-Experten, die 24x7x365 auf Abruf bereitstehen. Mit einer nachgewiesenen mittleren Lösungszeit von weniger als 20 Minuten können sie dazu beitragen, die Betriebseffizienz zu steigern und die Zahl der Kundeneinsätze zu erhöhen, ohne dass Sie mehr Personal einstellen müssen.

Erfahren Sie, wie N-able Managed EDR powered by SentinelOne Vigilance Ihnen helfen kann, die Herausforderungen von heute zu meistern und gleichzeitig Ihr Unternehmenswachstum zu beschleunigen. Weitere Einzelheiten finden Sie auf n-able.com/de.

[8]https://www.cyberseek.org/heatmap.html (Zugriff Dezember 2022)

N-able

N-able bietet MSPs und IT-Serviceanbietern leistungsstarke Software zur Überwachung, Verwaltung und Absicherung von IT-Infrastrukturen und Netzwerken. Unser Angebot umfasst eine skalierbare Plattform, eine sichere Infrastruktur, Tools für die einfachere Verwaltung komplexer IT-Umgebungen und Ressourcen für die digitale Transformation. Wir unterstützen unsere Partner in jeder Wachstumsphase beim Schutz ihrer Kunden sowie beim Ausbau ihres Angebots – durch das ständig wachsende flexible Portfolio an Integrationen führender Anbieter. n-able.com/de