Eine Studie von Forrester zum
Total Economic Impact™
im Auftrag von Arctic Wolf
Mai 2020

Total Economic Impact™ von Arctic Wolf Security Operations Solutions

Durch den Einsatz von Arctic Wolf erzielbare Kosteneinsparungen und Geschäftsvorteile

FORRESTER®

Inhaltsverzeichnis

Projektleitung:
Henry Huang

INFORMATIONEN ZU FORRESTER CONSULTING

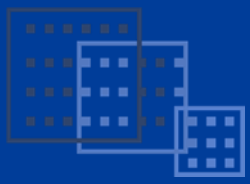
Forrester Consulting bietet unabhängige und objektive, auf Forschungsergebnisse gestützte Beratungsdienstleistungen und hilft Führungskräften dabei, ihre Unternehmen zum Erfolg zu führen. Die Beratungsdienste von Forrester reichen von kurzen Strategiesitzungen bis hin zu kundenspezifischen Projekten. Im direkten Austausch mit Ihnen unterstützen Forschungsanalytiker Sie mit ihrem Fachwissen bei Ihren spezifischen geschäftlichen Herausforderungen. Weitere Informationen finden Sie unter forrester.com/consulting.

FORRESTER®

Die wichtigsten Vorteile

Verringerung des Sicherheits- und IT-Aufwands beim Umgang mit Sicherheitsvorfällen:
556.677 $

Schnellere Wertschöpfung mit Arctic Wolf:
966.888 $



Eingesparte Software- und Infrastrukturkosten bei identischem Sicherheitsniveau:
1.415.505 $

Zusammenfassung

Die von Arctic Wolf als Managed Services angebotenen Security Operations optimieren die Abwehrstrategien von Unternehmen und stärken damit ihren Sicherheitsstatus. Fest zugewiesene Security Consultants unterstützen beim Kunden für IT und Sicherheit verantwortliche Teams und stehen ihnen bei ihrer Arbeit zur Seite. Hierfür greifen sie auf die cloudnative Arctic Wolf™ Platform zurück. Zu den angebotenen Leistungen zählen: Managed Detection and Response (MDR; verwaltete Bedrohungserkennung und -abwehr), Managed Risk (kontinuierliches Schwachstellenmanagement) sowie Managed Cloud Monitoring (Überwachung von Cloudinfrastrukturen und SaaS). Arctic Wolf hat Forrester Consulting mit der Durchführung einer Studie zum Total Economic Impact™ (TEI) sowie mit der Untersuchung der potenziell erzielbaren Kapitalrendite (Return on Investment, ROI) durch den Einsatz von Security Operations Services beauftragt. Die vorliegende Studie soll Lesern, die sich für die Lösungen von Arctic Wolf interessieren, eine Rahmenstruktur zur Beurteilung der potenziellen finanziellen Auswirkungen von Security Operations Services und des möglichen Effekts auf die Cybersicherheit im Unternehmen bereitstellen.

Um den Nutzen, die Kosten und die Risiken in Verbindung mit dieser Investition besser zu verstehen, hat Forrester zwei Kunden zu ihren umfassenden Erfahrungen mit zwei Security Operations Services von Arctic Wolf befragt: MDR und Managed Risk. Unsere Ergebnisse zeigen, dass die umfassende Absicherung über mehrere Cybersicherheitssegmente hinweg in zweierlei Hinsicht hilfreich war:

- Mit den Security Operations Services lässt sich das Leistungspotenzial der vorhandenen Sicherheitsinfrastruktur endlich vollständig ausschöpfen. Ohne Arctic Wolf wurden aufgezeichnete Protokolle beispielsweise nicht ausgewertet, da es an Mitarbeitern für forensische Untersuchungen mangelte. In einem anderen Fall wurde die Implementierung von SOAR (Security Orchestration Automation and Response) aufgrund von Lücken in der Sicherheitsgruppe gar nicht genutzt.
- Security Operations Services integrieren sich in gestraffte Prozesse und Arbeitsabläufe dieser Unternehmen und erweitern und verbessern so die Fähigkeiten der internen Sicherheitsteams. Die für das Thema Sicherheit zuständigen personellen Kapazitäten lassen sich jetzt einfach erweitern. Dadurch entfällt die mühsame Suche nach qualifizierten Experten und deren zeitaufwändige Schulung. Mit Arctic Wolf konnten Unternehmen mehr erreichen, ohne interne Ressourcen zu überlasten.

Vor der Zusammenarbeit mit Arctic Wolf konnten die befragten Kunden aufgrund begrenzter Personalressourcen keinen vollständigen Nutzen aus ihren Sicherheitsinvestitionen ziehen. Außerdem fiel es ihnen schwer zu erkennen, welche der zahlreichen von diesen Tools erkannten sicherheitsrelevanten Ereignisse echte Gefahren darstellten. Ein Befragter erklärte: „Arctic Wolf filtert aus Milliarden von Ereignissen insgesamt 15 Eskalationen heraus, die wir tatsächlich überprüfen müssen. Die damit verbundene Zeitersparnis ist enorm?“

Wesentliche Ergebnisse

Quantifizierter Nutzen. Das befragte Unternehmen profitierte von folgendem risikobereinigten quantifizierten Nutzen (Barwert):

FORRESTER®

ROI
411 %

Nutzen (Barwert)
2,9 Mio. $

KW
2,3 Mio. $

Amortisierung
< 6 Monate

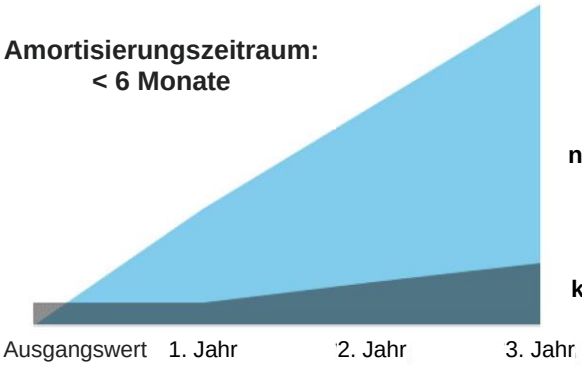
- **Da sich Sicherheitsvorfälle mit geringerem Aufwand beheben lassen, gewinnen Security- sowie IT-Mitarbeiter Zeit. Dadurch müssen Unternehmen keine weiteren Sicherheitsexperten einstellen.** Als verlängerter Arm eines SOC nimmt Arctic Wolf den internen Sicherheitsteams einen großen Teil ihrer Arbeit ab. Wachsende, jedoch in Sachen Ressourcen beschränkte Unternehmen, die auf bessere Erkennungs- und Abwehrmöglichkeiten angewiesen sind, profitieren wie folgt von der Zusammenarbeit mit Arctic Wolf: 1) Der für das interne Sicherheitsteam mit Analysen, Bewertungsprozessen (Triage) und Untersuchungen verbundene Aufwand sinkt um 50 Prozent. 2) 90 Prozent der im Zusammenhang mit dem Vorfallsmanagement stehenden IT-Prozesse entfallen. Dies führt in einem Zeitraum von drei Jahren zu Einsparungen in Höhe von 557.000 US-Dollar (BW).
- **Durch die Inanspruchnahme der Security Operations Services von Arctic Wolf konnten die Kosten in erheblichem Umfang gesenkt werden. Die Inbetriebnahme der Lösung – auch bei den Auftragnehmern – ließ sich in kürzerer Zeit durchführen, sodass sich die Investition schneller amortisierte.** Die Einrichtung herkömmlicher Einzellösungen erfordert Know-how und gestaltet sich aufwändig. Hierfür müssen häufig professionelle Dienstleistungen eingekauft, Lieferanten hinzugezogen oder weitere Vollzeitmitarbeiter eingestellt werden. Dies kostet Zeit und Geld. Das Baselining und die Überführung in einen stabilen und effizienten Systembetrieb nimmt bei einer herkömmlichen SIEM-Lösung samt zugehörigen Protokollierungstools im besten Fall etwa zehn Monate in Anspruch. Arctic Wolf ist bereits nach einem Monat einsatzbereit. Durch den geringeren Aufwand lässt sich der Einsatz weiterer Mitarbeiter vermeiden und Zeit sparen. Dadurch lassen sich die Ausgaben über drei Jahre hinweg um 967.000 US-Dollar (BW) senken.
- **Arctic Wolf ersetzt Einzellösungen, die für die Umsetzung einer proaktiven Sicherheitsstrategie erforderlich wären. Die Anschaffung und Wartung der hierfür ansonsten nötigen Software- und Hardwareinfrastruktur lässt sich dadurch vermeiden.** Um ein vergleichbares Maß an Effizienz wie mit den von Arctic Wolf angebotenen Security Operations zu erreichen, ist Personal und Software nötig. Dies verursacht erhebliche Investitions- und Betriebskosten. Beispielsweise lassen sich mit dem Einsatz von Protokollierungssystemen für die Risikoermittlung nötige Informationen gewinnen. Ohne Arctic Wolf müsste jedoch ein komplettes Team für das manuelle Sortieren und Klassifizieren der Daten abgestellt werden. Die damit verbundenen Einsparungen belaufen sich über einen Zeitraum von drei Jahren auf 1,4 Mio. US-Dollar (BW).

Kosten. Dem befragten Unternehmen entstanden die folgenden risikobereinigten, barwertigen Kosten.

- **Direkte Kosten der Security Operations Services von Arctic Wolf.** Die Kosten für die von Arctic Wolf erbrachten Dienstleistungen basieren unter anderem auf der Zahl der Nutzer und überwachten Assets – zum Beispiel Servern. Im Verlauf einer dreijährigen Bewertung entstehen Kosten mit einem Barwert von 575.000 US-Dollar. Den Annahmen zufolge fallen intern keine indirekten Kosten an.

Forresters Befragung von zwei Bestandskunden sowie die darauffolgende Finanzanalyse ergaben, dass den Unternehmen ein Gewinn von 2,9 Mio. US-Dollar im Vergleich zu Kosten von 575.000 US-Dollar entstand. Die Berechnung erfolgte als Kapitalwert (KW) bezogen auf einen Zeitraum von drei Jahren und ergab einen KW von 2,3 Mio. US-Dollar und eine Kapitalrendite (ROI) von 411 %.

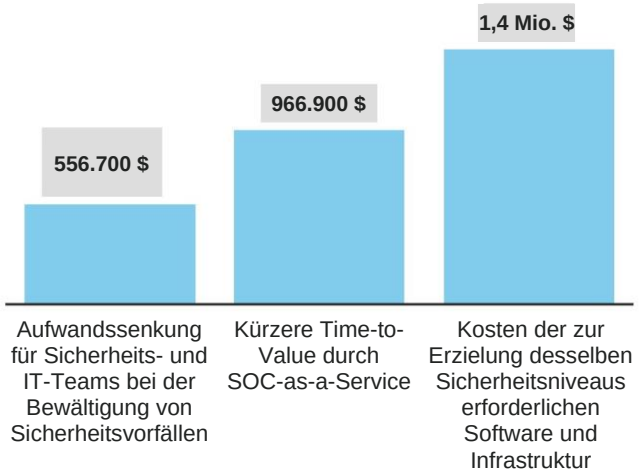
Zusammengefasste Finanzergebnisse



Gesamt-nutzen (BW): 2,9 Mio. $

Gesamt-kosten (BW): 575.000 $

Nutzen (über drei Jahre)



FORRESTER®

Total Economic Impact – Rahmenstruktur und Methodik

Aus den in der Befragung erfassten Daten erstellte Forrester eine TEI-Rahmenstruktur (Total Economic Impact™) für Unternehmen, die die Implementierung der Security Operations Services von Arctic Wolf in Erwägung ziehen.

Die Rahmenstruktur soll die Kosten, den Nutzen, die Flexibilität und die Risikofaktoren ermitteln, die die Investitionsentscheidung beeinflussen. Forrester verwendete ein mehrere Schritte umfassendes Verfahren, um die möglichen Auswirkungen der Security Operations Services von Arctic Wolf in einem Unternehmen zu bewerten.

Die TEI-Methodik erleichtert es Unternehmen, den messbaren Wert von IT-Initiativen gegenüber der oberen Führungsebene und anderen wichtigen geschäftlichen Stakeholdern zu demonstrieren, zu rechtfertigen und zu veranschaulichen.

SORGFALTSPFLICHT
Es wurden Stakeholder bei Arctic Wolf sowie Forrester-Analysten befragt, um Daten zur Nutzung der Security Operations Services zu erfassen.

KUNDENBEFRAGUNGEN
Um Daten in Bezug auf Kosten, Nutzen und Risiken zu erfassen, wurden zwei Unternehmen befragt, die Security Operations Services einsetzen.

FINANZMODELL
Anhand der TEI-Methodik wurde ein für die Befragung repräsentatives Finanzmodell erstellt und auf der Grundlage der Themen und Belange der befragten Unternehmen risikobereinigt.

FALLSTUDIE
Vier fundamentale Elemente von TEI bildeten die Grundlage der Modellierung von Auswirkungen der Security Operations Services von Arctic Wolf: Nutzen, Kosten, Flexibilität und Risiken. Angesichts der zunehmenden Komplexität, die Unternehmen in Bezug auf Kapitalrenditeanalysen im Zusammenhang mit IT-Investitionen erkennen, dient die TEI-Methodik von Forrester dazu, ein vollständiges Bild der gesamten wirtschaftlichen Auswirkungen von Kaufentscheidungen zu liefern. Weitere Informationen zur TEI-Methodik finden Sie in Anhang A.

FORRESTER®

Arctic Wolf: Customer Journey

VOR UND NACH DER INVESTITION IN SECURITY OPERATIONS SERVICES

Befragte Unternehmen

Für die vorliegende Studie befragte Forrester zwei Kunden, die die Plattform von Arctic Wolf und die zugehörigen Lösungen seit über einem Jahr nutzen. Die Unternehmen weisen die folgenden Eigenschaften auf:

- Beim ersten Unternehmen handelt es sich um eine Regionalbank in den USA, die einer umfassenden aufsichtsrechtlichen Kontrolle unterliegt und eindeutig einen Cybersicherheitsbedarf hat. Diese wachsende Bank mit mehreren Standorten ist nicht in der Lage, Sicherheitsabläufe so zu skalieren, dass sie mit dem Wachstum und dem Regulierungsdruck Schritt halten können. Die von Forrester durchgeführte Finanzanalyse unterstreicht die Erkenntnisse, die aus den Angaben dieses Unternehmens gewonnen wurden.
- Das zweite Unternehmen ist eine der weltweit größten Anwaltskanzleien. Hier werden über 2.000 Endpunkte und mehr als 500 Server eingesetzt. Das Unternehmen beschäftigt ein kleines Security-Operations-Team. Arctic Wolf unterstützt dieses mit ergänzenden Leistungen. Vor der Inanspruchnahme der Services von Arctic Wolf bewertete dieses Unternehmen seinen eigenen Sicherheitsreifegrad auf einer Skala von 0 bis 10 mit 6.

Zentrale Herausforderungen

Die beiden befragten Kunden gaben an, dass die Wirksamkeit ihrer Sicherheitsprogramme vor allem durch den Mangel an geeigneten Ressourcen eingeschränkt wurde. Obwohl zahlreiche Sicherheitstools und -infrastrukturen zum Einsatz kamen, ließ sich aufgrund nur eingeschränkt zur Verfügung stehender personeller Ressourcen die Lücke bei den Absicherungs- und Abwehrmaßnahmen nicht schließen. Diese Unternehmen konnten oft nur reagieren, statt proaktiv Zeit in nötige Sicherheitsmaßnahmen zu investieren. Einige der Probleme, die von diesen Unternehmen genannt wurden, lassen sich wie folgt zusammenfassen:

- **Ohne entsprechende personelle Ressourcen lieferten die Investitionen in Sicherheitstools nicht die gewünschten Ergebnisse.** Sicherheitstools sind zwar unverzichtbar, aber die von diesen Systemen bereitgestellten Informationen führten nicht unbedingt zur korrekten Erkennung von Sicherheitsvorfällen. Denn um diese Daten intensiv auszuwerten, daraus konkrete Warnungen zu gewinnen und echte Bedrohungen zu erkennen, hätte mehr Personal eingestellt werden müssen. Dies kam nicht infrage, da nur wenige Sicherheitsfachkräfte zu finden sind, die Ermittlungs- und Triageaufgaben übernehmen können. Dies ist jedoch eine Voraussetzung, um die Leistungsfähigkeit der Sicherheitssysteme wirklich ausschöpfen zu können. Folglich bemängelten Führungsteams, dass sich die Plattformen nicht amortisierten. Das allerdings war auf den Mangel an Mitarbeitern zurückzuführen, die Warnmeldungen in ihrer Gesamtheit hätten prüfen und die ordnungsgemäße Klärung erkannter Probleme sicherstellen können.
- **Unvorhergesehene und ausufernde Kosten für Sicherheitstools waren schwer in den Griff zu bekommen.** Das befragte Finanzdienstleistungsunternehmen gab zu bedenken, dass viele Investitionsentscheidungen länger dauerten und mehr Personalressourcen erforderten als ursprünglich erwartet. Dies führte zu einem Anstieg der Investitions- und Betriebskosten, der schwierig abzuschätzen und abzusichern war. Der Vertreter dieses Unternehmens meinte dazu:

> „Das Entschlüsseln unserer Protokolle war ein totaler Fehlschlag. Wir haben nur die Hälfte der Protokolldateien herangezogen, die wir für einen aussagekräftigen Einblick gebraucht hätten, und von diesen gerade einmal 20 % aktiv im Blick behalten. Da dies alles manuell erledigt wurde, lag der erreichte Korrelationsgrad fast bei null.“
>
> *CSO, Finanzdienstleistungen*

> „Ich musste mich ganz allein im Unternehmen um die Sicherheit kümmern und hatte einfach nicht die Zeit, alles im Blick zu behalten und richtig zu konfigurieren. Und da kam Arctic Wolf ins Spiel.“
>
> *Global InfoSec Director, Anwaltskanzlei*

FORRESTER®

„Ich hatte [eine Plattform für das Schwachstellenmanagement] eingerichtet, um selbst fortlaufend nach Sicherheitslücken suchen zu können … Aber diese Plattform als ‚umständlich' zu bezeichnen wäre noch freundlich ausgedrückt. Die Berichterstellung war eine einzige Katastrophe und ich weiß nicht, wie viele Stunden ich damit verbracht habe, den Scanner zu konfigurieren und zu aktualisieren oder herauszufinden, welche Patches tatsächlich aufgespielt werden mussten."

- **Der zunehmende Sicherheitsreifegrad und der Einsatz entsprechender Tools trieben Integrations- und Anlaufkosten stetig in die Höhe.** Das wachsende Angebot an Sicherheitstools für Finanzdienstleister führte zu zwei Problemen:
    - Erstens nahm die Einführung neuer Lösungen viel Zeit in Anspruch. Interne Kräfte mussten eingearbeitet und die Umgebung musste für den Einsatz der Tools konfiguriert werden. Die indirekten Kosten von punktuellen Sicherheitslösungen ließen sich erst nach der Anschaffung oder zumindest nach einer umfassenden Pilotphase beziehungsweise im Rahmen einer Machbarkeitsstudie messen.
    - Zweitens mussten neue Tools ordnungsgemäß in die vorhandenen punktuellen Sicherheitslösungen integriert werden. Sonst wären die Vorteile der Automatisierung und Orchestrierung für das Unternehmen verloren gegangen. Wie könnte man angesichts der vielen Einzellösungen alle Informationen zentral zusammenführen und so die Effizienz steigern? Dies war eine kostspielige Aufgabe, die ein Zusammenwirken von SecOps, DevOps und externen Fachkräften erforderte.

„Jetzt können wir den Betrieb wirklich rund um die Uhr aufrechterhalten – ganz ohne jegliche Personalaufstockung. Ob Korrelation oder Überwachung: Nun ist für alles gesorgt."

CSO, Finanzdienstleistungen

Die wichtigsten Ergebnisse

Die Befragung zeigte, dass die Investition in Security Operations Services von Arctic Wolf folgende Vorteile bietet:

- **Dauerhafte Überwachung rund um die Uhr, ohne dass hierfür zusätzliches Personal eingestellt werden muss.** Das Arctic Wolf Concierge Security Team sorgt rund um die Uhr für Sicherheit. Für viele Unternehmen mit begrenzten Ressourcen ist es schwierig, ihre IT-Umgebung durchgängig abzusichern. Dies würde erfordern, dass Beschäftigte im Schicht- oder Bereitschaftsdienst arbeiten. Entscheiden sie sich für Arctic Wolf, können sie Sicherheitsvorfälle praktisch verzögerungsfrei bewältigen. Die internen Teams werden nur dann alarmiert, wenn es unbedingt notwendig ist. Da die Reaktionszeit nach Angaben der Befragten oft um mehr als 6 Stunden verkürzt werden kann, lassen sich Auswirkungen von Sicherheitsvorfällen außerhalb der normalen Arbeitszeiten minimieren.
- **Die Zentralisierung der Daten sorgte für bessere Informationen und mehr Transparenz und ermöglichte es, das Nutzerverhalten zu analysieren (User Behavioral Analytics, UBA).** Die Unternehmen beschrieben, dass die an zentraler Stelle zusammengeführten Informationen für die nötige Transparenz und Berichtsoptionen sorgten. Dies vereinfachte die Einhaltung von Vorschriften und insbesondere die Erbringung von Nachweisen erheblich. Die UBA-Komponente gewährte eine neue Perspektive auf die Frage, ob es sich bei den internen Aktivitäten im Netz um legitime Arbeitshandlungen oder etwas Widerrechtliches handelte. Der neue Blickwinkel auf alle Aktivitäten verringerte die Ermittlungsarbeit der internen Teams.

„Es gibt Tools, die wir intern hätten beschaffen müssen, um eine Überwachung in der von Arctic Wolf durchgeführten Weise umzusetzen – beispielsweise Traffic Analyzer, IPS und zusätzliche Firewalls. Alles wäre separat gelaufen. Jetzt aber versorgt uns Arctic Wolf mit allen relevanten Informationen, die wir nicht einmal mehr selbst filtern und auswerten müssen."

CSO, Finanzdienstleistungen

- **Arctic Wolf erleichterte die Automatisierung und Orchestrierung.** Durch Nutzung der Security Operations Services von Arctic Wolf haben die Unternehmen SOAR-Elemente direkt implementiert. Die Übergabe der Orchestrierung an das Arctic Wolf Concierge Security Team straffte Arbeitsabläufe und entlastete die internen Mitarbeiter zeitlich.
- **Die Verringerung des „Rauschens" – der Zahl der Warnmeldungen – um 60 Prozent ermöglichte, sich stärker auf Sicherheitsereignisse mit Handlungsbedarf zu konzentrieren.** Zusätzlich zur Durchsicht von mehr als 15 Milliarden Ereignissen und Terabytes an Protokollen pro Monat ließen sich diese Ereignisse dank der Nutzung der cloudnativen Plattform von Arctic Wolf und der Zusammenarbeit mit dem Concierge Security Team auf die relevantesten Vorfälle reduzieren. Dies verringerte den Arbeitsaufwand der internen SecOps- und IT-Teams. Die so gewonnene Zeit wurde anderweitig genutzt, um einen geschäftlichen Mehrwert zu erzielen.
- **Arctic Wolf erweiterte damit das Sicherheitsteam des Unternehmens.** Der Global InfoSec Director eines befragten Unternehmens erläuterte:

  „Man hat mir eine Menge Arbeit abgenommen. Nachdem ich den Experten von Arctic Wolf die erforderlichen Daten zur Verfügung gestellt hatte, entwickelten sie sich im Grunde zu einem ‚verlängerten Arm' meines Büros. Mittlerweile greife ich noch stärker auf sie zurück."

  Das Vertrauen zwischen den Befragten und Arctic Wolf war so groß, dass der einem Befragten zugewiesene Security Engineer am Ende genauso viel (wenn nicht sogar mehr) über das Innenleben des Kundennetzwerks wusste wie der Kunde selbst – ein Umstand, der für sich spricht.

> „Der größte Vorteil der Zusammenarbeit mit Arctic Wolf besteht darin, dass sich die Kosten im Griff behalten lassen. Wir wollten wissen, wie wir schrittweise skalieren können – ohne böses Erwachen. Wir müssen uns nicht länger darüber Gedanken machen, wie groß unsere Protokolldateien sind oder die Zahl der Nutzer ist. Wir sind uns über die Mehrkosten stets im Klaren und können die für uns erforderlichen Services abrufen, sobald wir sie benötigen."
>
> *CSO, Finanzdienstleistungen*

Nutzenanalyse

QUANTIFIZIERTE NUTZENDATEN

Gesamtnutzen

REF.	NUTZEN	1. JAHR	2. JAHR	3. JAHR	SUMME	BARWERT
Atr	Aufwandssenkung für Sicherheits- und IT-Teams bei der Bewältigung von Sicherheitsvorfällen	192.960 $	192.960 $	295.200 $	681.120 $	556.677 $
Btr	Kürzere Time-to-Value für Security Operations	388.800 $	388.800 $	388.800 $	1.166.400 $	966.888 $
Ctr	Kosten der zur Erzielung desselben Sicherheitsniveaus erforderlichen Software und Infrastruktur	589.498 $	557.498 $	557.498 $	1.704.493 $	1.415.505 $
	Gesamtnutzen (risikobereinigt)	1.171.258 $	1.139.258 $	1.241.498 $	3.552.013 $	2.939.070 $

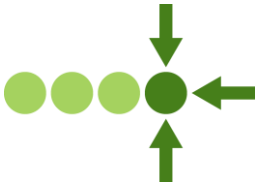
Die obige Tabelle zeigt die Summe des Gesamtnutzens in allen darunter aufgeführten Bereichen sowie Barwerte diskontiert mit 10 %. Über drei Jahre rechnet das befragte Unternehmen mit einem risikobereinigten Gesamtnutzen mit einem Barwert von mehr als 2,9 Mio. US-Dollar.

Aufwandssenkung für Sicherheits- und IT-Teams bei der Bewältigung von Sicherheitsvorfällen

Das Finanzdienstleistungsunternehmen konstatierte vor allem einen drastischen Rückgang des Arbeitsaufwands für die internen Mitarbeiter – genau das, was die Security Operations Services von Arctic Wolf bezwecken sollten. Dies betraf im Wesentlichen zwei Gruppen:

- SecOps-Fachkräfte, die in der Regel die erste Verteidigungslinie bilden und mit der Erkennung und Untersuchung von Sicherheitsvorfällen sowie Triage und Problembehebung befasst sind.
    - Ein Hauptgrund für die Reduzierung war die Beseitigung des Rauschens: Es wurden nur noch Vorfälle angezeigt, die Relevanzkriterien erfüllten. Probleme ließen sich dadurch schneller und ohne große Mühe ermitteln.
    - Die Qualität der verfügbaren Kontextinformationen erleichterte zudem Überprüfungs- und Bewertungsprozesse sowie die Planung von Abwehrmaßnahmen. Die bereitgestellten Informationen waren weder generisch noch spezifisch auf die Netzmerkmale des jeweiligen Unternehmens beschränkt.
    - Die weltweit tätige Anwaltskanzlei gab an, dass die Zahl der Fehlalarme in Folge der Zusammenarbeit mit Arctic Wolf um 60 Prozent zurückging. Dies ermöglichte dem internen SecOps-Team, sich entscheidenderen Aufgaben zuzuwenden.
    - Arctic Wolf führte die Ermittlung und Eindämmung von Problemen so lange automatisiert durch, bis diese eskaliert werden mussten. Praktisch alle Elemente wurden durch Arctic Wolf orchestriert.
- IT-Verantwortliche, die zudem als Incident Responders fungieren, spielen bei der Durchführung von Abwehrmaßnahmen und der Fehlerbehebung eine wichtige Rolle. Arctic Wolf wurde von den befragten Unternehmen als Partner beschrieben, der zu ergreifende Abwehrmaßnahmen „auf dem Silbertablett serviert“, insofern das Arctic Wolf Concierge Security Team diese nicht bereits umgesetzt hat. Daraus resultierend verringerte sich für viele Incident Responders der Aufgabenumfang um 90 Prozent, sodass sie sich wertschöpfenderen IT-Projekten zuwenden konnten.

Das vorgestellte Modell enthält einige Annahmen zur Zeitersparnis, die eng an die Arbeitsweise des befragten Finanzdienstleistungsunternehmens angelehnt sind.



Arctic Wolf behebt einen Großteil der Vorfälle selbst und übergibt nur wenige davon an das interne Incident-Response-Team, das sich dadurch vollständig auf diese konzentrieren kann.

FORRESTER®

- Die SecOps-Gruppe besteht zunächst primär aus einer Person, wird aber im Laufe der Zeit erweitert. Dadurch kann sie sich anspruchsvolleren Aufgaben wie dem Threat Hunting widmen.
- Der SecOps-Mitarbeiter konzentriert sich auf Arbeitsabläufe, die der Abwehr und Beseitigung von Bedrohungen dienen. Da jedoch Arctic Wolf den Großteil dieser Arbeit übernimmt, geht der hierfür bislang erforderliche manuelle Aufwand enorm zurück.

Schlüsselt man die Berechnungen weiter auf, sollte auf Basis der vom Finanzinstitut mitgeteilten Informationen Folgendes unbedingt beachtet werden:

- SecOps-Mitarbeiter kümmern sich in der Regel um das Management, die Berichterstattung oder die Bedrohungsabwehr. Letztere Aufgabe beansprucht einen Großteil ihrer Zeit.
- Das IT-Betriebspersonal des Unternehmens wendet 40 % seiner Zeit für sicherheitsrelevante Vorfälle auf, insbesondere für Absicherung und Abwehr.
- Viele Sicherheitsvorfälle werden erfolgreich von dem Arctic Wolf Concierge Security Team behoben. Das senkt den Aufwand für Kunden erheblich. Die verbleibenden Ereignisse, die weiterhin Aufmerksamkeit erfordern, werden mit den nötigen und eindeutigen Kontextinformationen als Maßnahme an das IT- oder SecOps-Team übermittelt.

All dies berücksichtigend, geht Forrester davon aus, dass die durch schlanke SecOps- und IT-Teams in drei Jahren erzielbare Zeitersparnis einem Barwert in Höhe von 556.677 US-Dollar entspricht.

Die Zahl der Vorfälle, denen tatsächlich weiterhin Aufmerksamkeit geschenkt werden muss, nimmt immens ab. Das führt dazu, dass Überprüfungs- und Bewertungsprozesse entfallen.

Aufwandssenkung für Sicherheits- und IT-Teams bei der Bewältigung von Sicherheitsvorfällen: Berechnungstabelle

REF.	KENNZAHL	BERECHNUNG	1. JAHR	2. JAHR	3. JAHR
A1	Anzahl der SecOps-VZÄ		1	1	2
A2	Geringerer SecOps-Aufwand für die Überprüfung, Bewertung und Behebung von Sicherheitsvorfällen	Verringerung des SecOps-Aufwands (in %)	50 %	50 %	50 %
A3	Jahresgehalt SecOps-Mitarbeiter (Gesamtlohnkosten)	120.000 $*1,2X (Faktor Zusatzleistungen)	144.000 $	144.000 $	144.000 $
A4	Anzahl der IT-VZÄ		4	4	5
A5	Zeitaufwand der IT bei sicherheitsrelevanten Vorfällen		40 %	40 %	40 %
A6	Für die IT sicherheitsrelevanter Vorfall, der von Security Operations abgefangen wurde		90 %	90 %	90 %
A7	Jahresgehalt (inkl. Nebenkosten) für IT-Mitarbeiter	70.000 $*1,2X (Faktor Zusatzleistungen)	84.000 $	84.000 $	84.000 $
At	Aufwandssenkung für Sicherheits- und IT-Teams bei der Bewältigung von Sicherheitsvorfällen	(A1*A2*A3)+ (A4*A5*A6*A7)	192.960 $	192.960 $	295.200 $
	Risikobereinigung	0 %			
Atr	Aufwandssenkung für Sicherheits- und IT-Teams bei der Bewältigung von Sicherheitsvorfällen (risikobereinigt)		192.960 $	192.960 $	295.200 $

Kürzere Time-to-Value für Security Operations bei Verwendung von Arctic Wolf

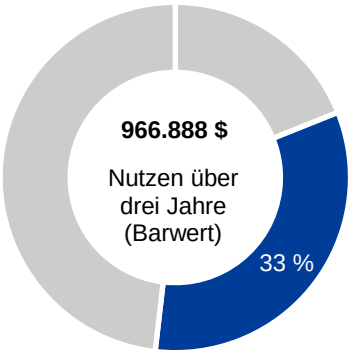
Für das von Forrester befragte Finanzdienstleistungsunternehmen war es entscheidend, sofort einen Mehrwert realisieren zu können. Das Unternehmen hatte zuvor mit mehreren Lösungen experimentiert, bei denen sich Bereitstellung, Integration und Baselining lange hinzogen und eine Einarbeitungsphase für die Mitarbeiter nötig war. Angesichts der sich in raschem Tempo weiterentwickelnden Sicherheitsprodukte suchte es nach einer Lösung, die einen schnellen Mehrwert bot. Eine langwierige Einführung würde dazu führen, dass das Unternehmen sich gegenüber der wachsenden Zahl böswilliger Akteure im Nachteil befindet. Die Security Operations Services von Arctic Wolf ließen sich in kürzester Zeit einführen. Die Einrichtung einschließlich Baselining und Integration des vorhandenen Sicherheitsstacks nahm weniger als einen Monat in Anspruch. Dies sicherte einen nahtlosen und unkomplizierten Umstieg.

Forrester nimmt für das befragte Unternehmen Folgendes an:

- Zur Echtzeiterfassung von Daten implementiert das Unternehmen zahlreiche für Arctic Wolf verfügbare Integrationen von Plattformen wie etwa Endpoint Detection and Response (EDR), Firewalls und verschiedenen Protokollierungssystemen. Diese Integrationen werden von Arctic Wolf vorgenommen.
- Baselining und die Anbindung an das lokale Netzwerk erfolgen durch Arctic Wolf im Rahmen eines umfangreichen Einführungsprozesses, der etwa einen Monat dauert.
- Die Einführung und Einrichtung alternativer Lösungen wie SIEM-Software (Security Information and Event Management) und zusätzlicher Protokollierungsprogramme würde aufgrund der Einarbeitungszeit in die Tools einen erheblichen Personalaufwand bedeuten. In Summe wären drei zusätzliche SecOps-Fachkräfte nötig. Dabei spielt es keine Rolle, ob es sich um unabhängige, auf eigene Rechnung arbeitende Vertragspartner oder Vollzeitmitarbeiter handelt.
- Der Einkauf professioneller Dienstleister oder die Beauftragung Dritter für die Implementierung wäre kostspieliger und wird daher bei alternativen Lösungen meist vermieden.

SIEM und die Protokollanalyse sind für Unternehmen, die über ausgereifte Sicherheitsprogramme verfügen, von grundlegender Bedeutung. Forrester berücksichtigte dies in der Studie und bezog sie in die Analyse ein. Solche Tools werden beispielsweise vom befragten Finanzdienstleistungsunternehmen benötigt. Die Bereitstellung und Inbetriebnahme der Lösung von Arctic Wolf nahm lediglich einen Monat in Anspruch. Bei einer einzelnen Lösung können hingegen zehn Monate ins Land ziehen, bis konkrete Ergebnisse erzielt werden.

SIEM- und Protokollierungstools unterscheiden sich hinsichtlich ihrer Komplexität. Dies kann sich auf den Aufwand auswirken, der für die Einrichtung eines wettbewerbsfähigen SIEM-Tools erforderlich ist. Daher hat Forrester diesen Nutzen um 10 % nach unten korrigiert. Daraus resultiert ein risikobereinigter Dreijahresgesamtbarwert in Höhe von 966.888 US-Dollar.



Kürzere Time-to-Value mit Arctic Wolf: 33 % des Gesamtnutzens

Die Time-to-Value beträgt bei Arctic Wolf nur einen Monat, bei einer herkömmlichen SIEM- oder Protokollierungslösung hingegen zehn Monate.

Hinter dem Begriff „Folgerisiko“ verbirgt sich das Risiko, dass eine Investition die geschäftlichen oder technischen Anforderungen des Unternehmens nicht erfüllt. Das schränkt den Gesamtnutzen ein. Je größer die Unsicherheit, desto stärker variieren die Ergebnisse der Nutzeneinschätzung.

FORRESTER®

Kürzere Time-to-Value für Security Operations: Berechnungstabelle					
REF.	**KENNZAHL**	**BERECHNUNG**	**1. JAHR**	**2. JAHR**	**3. JAHR**
B1	Mit SIEM und Protokollanalysen befasste SecOps-Mitarbeiter		1	1	1
B2	Für den Betrieb alternativer SIEM- und Protokollanalysetools erforderliche zusätzliche SecOps-Mitarbeiter		3	3	3
B3	Bereitstellungszeit von Arctic Wolf Security Operations	Angabe in Monaten	1	1	1
B4	Bereitstellungszeit für SIEM und Protokollierungssystem	Angabe in Monaten	10	10	10
B5	Kosten je SecOps-VZÄ pro Jahr (Gesamtlohnkosten)	120.000 $*1,2X (Faktor Zusatzleistungen)	144.000 $	144.000 $	144.000 $
Bt	Kürzere Time-to-Value für Security Operations bei Verwendung von Arctic Wolf	(B4-B3)/12*(B1+B2)*B5	432.000 $	432.000 $	432.000 $
	Risikobereinigung	↓ 10 %			
Btr	Kürzere Time-to-Value für Security Operations bei Verwendung von Arctic Wolf (risikobereinigt)		388.800 $	388.800 $	388.800 $

Kosten der zur Erzielung desselben Sicherheitsniveaus erforderlichen alternativen Software und Infrastruktur

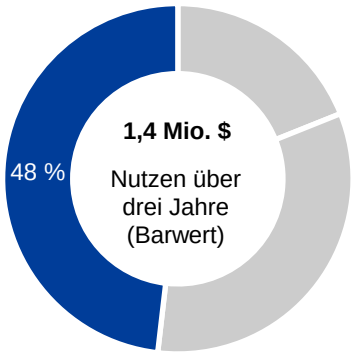
Die befragten Unternehmen gaben an, dass zusätzliche Software-, Infrastruktur- und Personalressourcen für den Betrieb dieser Assets erforderlich wären, um ein mit Arctic Wolf vergleichbares Abwehrniveau zu erreichen. Einer der wesentlichen Gründe gegen die Entscheidung für eine alternative Variante waren die damit verbundenen ausufernden Kosten. Um ein Sicherheitsniveau zu erreichen, das dem von Arctic Wolf nahekommt, ist der Einsatz zusätzlicher separater Softwarelösungen erforderlich – und das manchmal in beträchtlicher Zahl. Hierzu zählen unter anderem ein vorschriftsmäßiges SIEM, ein Intrusion Prevention System (IPS), SOAR und verschiedene Netzwerk-Analyzer.

Die Ausgaben für diese Geräte und die Software sind bereits beachtlich. Des Weiteren ist die Einstellung zusätzlicher Sicherheitsfachkräfte erforderlich. Diese zu finden stellt ebenso eine Herausforderung dar wie die Bewältigung der mit ihrer Beschäftigung verbundenen Zusatzkosten. Um mit diesen zusätzlichen Sicherheitskomponenten ein Sicherheitsniveau zu erreichen, das dem von Arctic Wolf nahekommt, sind weitere Mitarbeiter nötig. Forrester schätzt den Personalbedarf wie folgt ein:

- Drei SecOps-Mitarbeiter sind vor allem dann erforderlich, wenn Ermittlungen auf Protokollebene einen hohen Stellenwert haben. Darüber hinaus sind die SIEM-Überwachung und die Datenkonsolidierung Aufgaben, für die diese Vollzeitkräfte zuständig wären.
- Zwei IT-Vollzeitkräfte werden für Wartung, Überwachung und Unterstützung der verschiedenen Punktlösungen benötigt.

Allein diese zusätzliche Infrastruktur kostet im ersten Jahr schätzungsweise 137.000 US-Dollar. Über drei Jahre summieren sich diese Kosten auf 330.000 US-Dollar. Wenn man das für die Unterstützung dieser Infrastruktur erforderliche Personal einbezieht, steigen die Kosten auf bis zu 1,76 Mio. US-Dollar (BW) über drei Jahre.

Da die Ausgangssituation in den Unternehmen unterschiedlich ist, kann die jeweilige Höhe der Einsparungen variieren. Um dies zu berücksichtigen, korrigierte Forrester den Nutzen um 20 % nach unten. Dies ergibt über einen Zeitraum von drei Jahren einen risikobereinigten Gesamtbarwert (BW) in Höhe von 1.415.505 US-Dollar.



Kosten der zur Erzielung desselben Sicherheitsniveaus erforderlichen alternativen Software und Infrastruktur: 48 % des Gesamtnutzens

Kosten der zur Erzielung desselben Sicherheitsniveaus erforderlichen alternativen Software und Infrastruktur: Berechnungstabelle

REF.	KENNZAHL	BERECHNUNG	1. JAHR	2. JAHR	3. JAHR
C1	Kosten für Nutzer und Assets in ähnlichem Umfang einer alternativen SIEM-Lösung (nicht MDR)		16.872 $	16.872 $	16.872 $
C2	Zusätzlicher SecOps-Arbeitsaufwand für den Betrieb der Lösung (nicht MDR)	3 VZÄ* 144.000 $/Jahr	432.000 $	432.000 $	432.000 $
C3	Zusätzlicher IT-Arbeitsaufwand für den Betrieb der alternativen Lösung (nicht MDR)	2 VZÄ* 84.000 $/Jahr	168.000 $	168.000 $	168.000 $
C4	Kosten für Software und Infrastruktur, ohne SIEM		120.000 $	80.000 $	80.000 $
Ct	Kosten der zur Erzielung desselben Sicherheitsniveaus erforderlichen alternativen Software und Infrastruktur	C1+C2+C3+C4	736.872 $	696.872 $	696.872 $
	Risikobereinigung	↓ 20 %			
Ctr	Kosten der zur Erzielung desselben Sicherheitsniveaus erforderlichen alternativen Software und Infrastruktur (risikobereinigt)		589.498 $	557.498 $	557.498 $

FORRESTER®

Flexibilität

Flexibilität besitzt für jeden Kunden einen anderen Wert. Wie dieser bemessen wird, variiert von Unternehmen zu Unternehmen. Es gibt mehrere Szenarien, in denen sich ein Kunde für die Einführung von Arctic Wolf entscheidet und erst später weitere Anwendungsmöglichkeiten und Chancen erkennt. Hierzu zählt beispielsweise:

- **Die organische oder durch Fusionen und Übernahmen bedingte Erweiterung des Sicherheitsstacks kann in den meisten Fällen ohne Zusatzkosten von Arctic Wolf übernommen werden.** Eine höhere Standortdichte führt typischerweise zu einer umfangreicheren Netz- und Sicherheitsinfrastruktur, in der mehr Daten erzeugt werden. Um zusätzliche Sicherheitsebenen zu schaffen, ist zudem der Einsatz weiterer Sicherheitstools zwingend erforderlich. Zwar fallen für die zur Erfassung des Datenflusses notwendigen Sensoren Kosten an, jedoch nicht für die Integration.
- **Eine zentrale Managementkonsole erleichtert es, Compliance-Vorgaben einzuhalten und die Vielzahl an Rechtsvorschriften im Griff zu behalten.** Das befragte Finanzunternehmen war daran gewöhnt, zahlreiche Regulierungsmaßnahmen einhalten zu müssen. Wächst ein Unternehmen, muss es häufig weitere Compliance-Vorgaben einhalten. Hierzu zählt beispielsweise der für alle börsennotierten Firmen vorgeschriebene Sarbanes-Oxley Act (SOX). Sowohl beim California Consumer Privacy Act (CCPA) als auch beim Payment Card Industry Data Security Standard (PCI-DSS) sind die Kontrollen umso rigider, je größer die Standortdichte des betreffenden Unternehmens ist. Alle Informationen sind in der Managementkonsole von Arctic Wolf zentralisiert verfügbar. Dies macht eine frühzeitige Berichterstattung über die Einhaltung von Vorschriften möglich und verringert selbst bei schnellem Wachstum den Prüfungsaufwand des Unternehmens.

Flexibilität lässt sich auch quantifizieren, wenn sie als Teil eines konkreten Projekts bewertet wird (weitere Informationen finden Sie in Anhang A).

Flexibilität stellt gemäß Definition der TEI-Methodik eine Investition in eine zusätzliche Kapazität oder Fähigkeit dar, die sich in einen Geschäftswert einer weiteren künftigen Investition umsetzen lässt. Dies räumt dem Unternehmen das „Recht“ beziehungsweise die Möglichkeit ein, sich an zukünftigen Initiativen zu beteiligen. Das Unternehmen ist jedoch zu nichts verpflichtet.

Kostenanalyse

QUANTIFIZIERTE KOSTENDATEN

Gesamtkosten

REF.	KOSTEN	ANFANGS-WERT	1. JAHR	2. JAHR	3. JAHR	SUMME	BARWERT
Dtr	Direkte Kosten von Arctic Wolf Security Operations	213.300 $	0 $	223.965 $	235.164 $	672.429 $	575.077 $
	Gesamtkosten (risikobereinigt)	213.300 $	0 $	223.965 $	235.164 $	672.429 $	575.077 $

Die obige Tabelle zeigt die Summe aller Kosten in allen darunter aufgeführten Bereichen sowie die Barwerte (BW) diskontiert mit 10 %. Über drei Jahre rechnet das befragte Unternehmen mit risikobereinigten Gesamtkosten in einem Barwert von ca. 575.000 US-Dollar.

Direkte Kosten von Arctic Wolf Security Operations

Die Kosten, die dem befragten Finanzdienstleister für die Inanspruchnahme der Security Operations Services entstanden sind, basieren auf einigen einfachen von Arctic Wolf geprüften Faktoren. Es fielen keine zusätzlichen Kosten an, denn der Schulungsaufwand für die Lösung ist gering. Des Weiteren lässt sie sich einfach integrieren und an kundenspezifische Anforderungen anpassen, sodass die hiermit verbundenen internen Aufwendungen ebenfalls niedrig sind. Die Leser sollten beachten, dass die Kostenangaben auf den Listenpreisen basieren, um im Einklang mit der konservativen Analyse von Forrester zu bleiben.

Folgende Faktoren tragen zu den Kosten von Arctic Wolf Security Operations bei:

- Anzahl der verwalteten Unternehmensnutzer
- Anzahl der überwachten Server
- Anzahl der Sensoren und die von diesen genutzte Bandbreite
- Die vorliegende Kostenanalyse von Forrester berücksichtigt weder Managed-Risk- noch Managed-Cloud-Monitoring-Services. Die Preisgestaltung ist jedoch ähnlich.

Auf Grundlage der vom Kunden vorgelegten Informationen errechnete Forrester, dass dem Unternehmen über einen Zeitraum von drei Jahren geschätzt Kosten in Höhe von 383.385 US-Dollar (BW) entstehen. Allerdings ist zu beachten, dass die Diskrepanz bei Bandbreite und Sensoren selbst zwischen Unternehmen mit einer ähnlichen Nutzerzahl beträchtlich sein kann.

Angesichts der möglichen Schwankungsbreite dieser Faktoren und ihres potenziellen Einflusses auf die Endkosten hat Forrester diesen Wert um 50 % nach oben korrigiert und trägt damit den meisten denkbaren Situationen Rechnung. Über einen Zeitraum von drei Jahren ergibt sich ein risikobereinigter Gesamtbarwert von 575.077 US-Dollar.

Da stets nur die Zahl der abgesicherten Ressourcen die Basis für die Kosten bildet, lassen sich diese leicht im Griff behalten. Dies stellt eine Abkehr von den Prinzipien traditioneller Sicherheitsprogramme dar.

Unter dem Implementierungsrisiko versteht man das Risiko, dass eine vorgesehene Investition unter Umständen von den ursprünglichen oder erwarteten Anforderungen abweichen könnte. Dies führt zu höheren Kosten als angenommen. Je größer die Unsicherheit, desto stärker variieren die Ergebnisse der Kosteneinschätzung.

Direkte Kosten von Arctic Wolf Security Operations: Berechnungstabelle

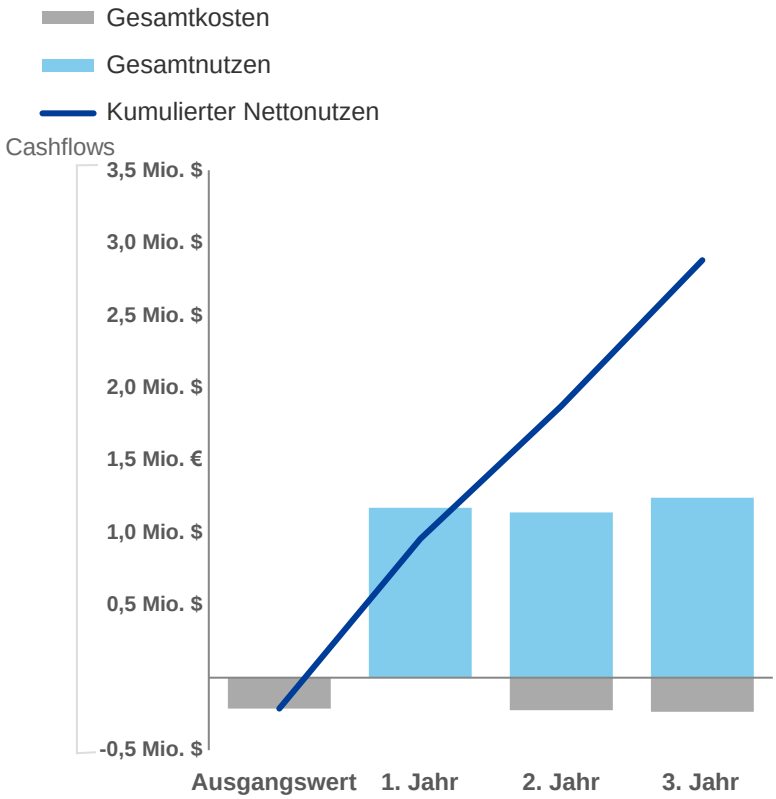
REF.	KENNZAHL	BERECHNUNG	ANFANGSWERT	1. JAHR	2. JAHR	3. JAHR
D1	Erfasste MDR-Nutzer		66.600 $		69.930 $	73.427 $
D2	Überwachte Server		3.600 $		3.780 $	3.969 $
D3	Überwachte Sensoren		72.000 $		75.600 $	79.380 $
Dt	Direkte Kosten von Arctic Wolf Security Operations	D1+D2+D3	142.200 $	0 $	149.310 $	156.776 $
	Risikobereinigung	↑ 50 %				
Dtr	Direkte Kosten von Arctic Wolf Security Operations (risikobereinigt)		213.300 $	0 $	223.965 $	235.164 $

FORRESTER®

Zusammengefasste Finanzergebnisse

KONSOLIDIERTE RISIKOBEREINIGTE DREIJAHRESKENNZAHLEN

Cashflow-Diagramm (risikobereinigt)



Die in den Abschnitten „Nutzen“ und „Kosten“ berechneten finanziellen Ergebnisse können zur Bestimmung des ROI, des Kapitalwerts und des Amortisierungszeitraums für die Investition des befragten Unternehmens herangezogen werden. Forrester hat dieser Analyse einen jährlichen Diskontsatz von 10 % zugrunde gelegt.

Für die Ermittlung der risikobereinigten Werte für ROI, KW und Amortisierungszeitraum werden Risiko-anpassungsfaktoren auf die unbereinigten Ergebnisse der einzelnen Nutzen- und Kosten-abschnitte angewendet.

Cashflow-Tabelle (risikobereinigt)

	ANFANGSWERT	1. JAHR	2. JAHR	3. JAHR	SUMME	BARWERT
Gesamtkosten	(213.300 $)	0 $	(223.965 $)	(235.164 $)	(672.429 $)	(575.077 $)
Gesamtnutzen	0 $	1.171.258 $	1.139.258 $	1.241.498 $	3.552.013 $	2.939.070 $
Nettonutzen	(213.300 $)	1.171.258 $	915.293 $	1.006.334 $	2.879.584 $	2.363.993 $
ROI						411 %
Amortisierungszeitraum						< 6 Monate

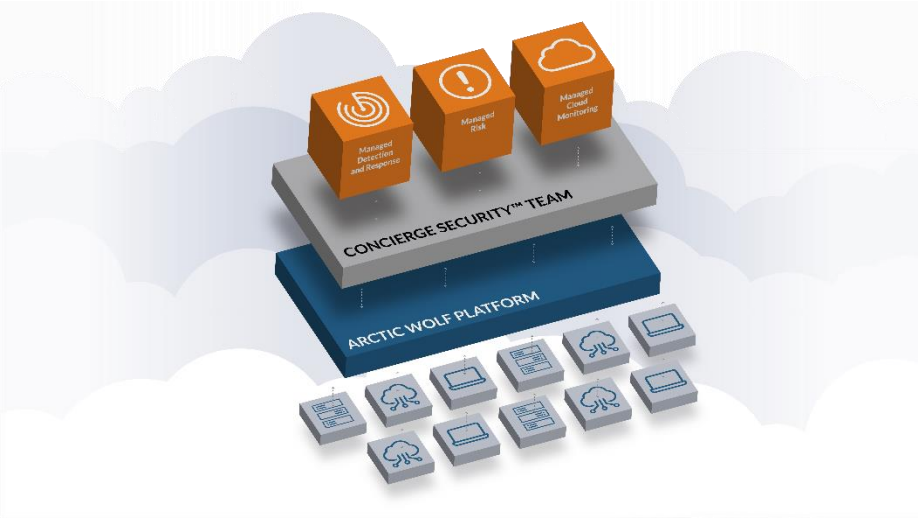
FORRESTER®

Arctic Wolf Security Operations: Übersicht

Die folgenden Informationen wurden von Arctic Wolf bereitgestellt. Forrester hat die Behauptungen nicht überprüft und empfiehlt weder Arctic Wolf noch seine Angebote.

Arctic Wolf Security Operations: Lösungsangebote

Arctic Wolf bietet drei Security-Operations-Lösungen an: Managed Detection and Response, Managed Risk und Managed Cloud Monitoring. Diese werden über die Plattform von Arctic Wolf bereitgestellt und als Concierge-Service angeboten.



Arctic Wolf Platform

Um heutige Bedrohungen erfolgreich abzuwehren, müssen riesige Datenmengen analysiert werden. Hierfür müssen von IT- und Sicherheitsprodukten Telemetriedaten gesammelt und so schnell wie möglich verarbeitet werden. Die meisten Unternehmen verfügen zwar über Tools, die diese Daten erzeugen. Allerdings sind sie nicht in der Lage, sie sinnvoll zu nutzen oder einen Mehrwert aus ihnen zu ziehen.

Arctic Wolf® stellt Security Operations über die cloudnative Arctic Wolf™ Platform bereit und bietet sie als Concierge-Service an. Während andere Systeme nur sehr eingeschränkte Einblicke zu nur wenigen Parametern bieten, kann die herstellerneutrale Plattform von Arctic Wolf im Zusammenspiel mit dem bestehenden Technologiestack des Unternehmens genutzt werden und täglich mehr als 60 Milliarden Sicherheitsereignisse in Netzwerken, an Endpunkten und in Cloudinfrastrukturen aufzeichnen. So lassen sich blinde Flecken erkennen und beseitigen.

Die Plattform wurde entwickelt, um Sicherheitsdaten in großem Stil zu sammeln, anzureichern und zu analysieren. Sie ist die Grundlage der Lösungen, die vom Concierge Security® Team (CST) bereitgestellt werden.

Concierge Security Team

Rund um den Globus sind Unternehmen gefordert, mit der beständig steigenden Zahl an Cyberangriffen und deren zunehmender Komplexität Schritt zu halten. Ziel ist es, Sicherheitsverletzungen, Datenverlusten und Ausfallzeiten vorzubeugen, die hohe Kosten verursachen können. Verschärft wird die Situation durch Alarmermüdung, fehlende standardisierte Prozesse und die Schwierigkeit, für eine unterbrechungsfreie Absicherung der IT-Umgebung erforderliche Cybersecurity-Experten zu gewinnen und zu halten.

Das Concierge Security® Team von Arctic Wolf verfügt über ein umfassendes Verständnis der individuellen IT-Umgebung des Kunden und überwacht diese auf sicherheitsrelevante Ereignisse. Die auf der Plattform von Arctic Wolf™ mit weiteren Daten angereicherten und analysierten Informationen werden dem meist nur aus wenigen Mitarbeitern bestehenden IT-Team beim Kunden im Anschluss bereitgestellt. Die speziell auf ihre individuellen Anforderungen zugeschnittene Berichterstattung, sicherheitstechnische Expertise und strategische Sicherheitsempfehlungen ermöglichen ihnen, den Sicherheitsstatus übergreifend und fortlaufend zu verbessern.

Managed Detection and Response

Rund um den Globus sind Unternehmen gefordert, aktuelle Cyberbedrohungen zu erkennen und durch die zeitnahe Einleitung von Gegenmaßnahmen erfolgreich abzuwehren. Zwar nutzen viele IT-Abteilungen Sicherheitstools, um diesem Problem entgegenzutreten. Meist können sie jedoch keine Absicherung rund um die Uhr gewährleisten. Hinzu kommt, dass es an umfassender Sicherheitsexpertise und einem personell gut besetzten Sicherheitsteam mangelt. Infolgedessen bleiben viele Bedrohungen unbemerkt und können sich über Monate hinweg in der IT-Umgebung festsetzen. Viele schwerwiegende Datenschutzverletzungen sind nicht darauf zurückzuführen, dass das Sicherheitstool keinen Alarm ausgelöst hat. Vielmehr blieb die Warnmeldung unbeachtet oder wurde übersehen.

Managed Detection and Response von Arctic Wolf™ basiert auf der branchenweit einzigen cloudnativen Plattform, die Security Operations in Form eines Concierge-Service bereitstellt. Die Lösung verhindert Fehlalarme sowie durch zu viele Alarme eintretende Gewöhnungseffekte. Die Folge sind schnellere Antwortzeiten dank passgenau auf die spezifischen Anforderungen des Kunden zugeschnittenen Erkennungs- und Reaktionsfunktionen. In enger Abstimmung mit dem Kunden spürt das zuständige Arctic Wolf Concierge Security® Team (CST) Bedrohungen auf, reagiert auf sicherheitsrelevante Vorfälle und behebt diese. Gleichzeitig spricht es aber auch strategische Empfehlungen aus, die auf die speziellen Anforderungen der Kundenumgebung zugeschnitten sind.

Managed Risk

Überall kämpfen IT-Abteilungen mit der immer komplexeren Aufgabe, potenzielle Sicherheitsrisiken zu erkennen und zu bewältigen. Oftmals ist es nahezu unmöglich, grundlegende Informationen zu den in der Umgebung vorhandenen Assets oder schwachstellenbehafteten beziehungsweise fehlerhaft konfigurierten Systemen zu erhalten. Selbst wenn diese Informationen vorliegen, ist das Sicherheitsteam hiervon meist überfordert. Dies liegt im Wesentlichen daran, dass die eingesetzten Sicherheitstools zu viele Warnmeldungen ausgeben und der Kontext fehlt. Während sich die Teams mit der Frage auseinandersetzen, was als Nächstes zu tun ist und welche Prioritäten zu setzen sind, häufen sich diese Risiken und machen das Unternehmen anfällig für Bedrohungen und Datenschutzverstöße mit hohem Schadenspotenzial.

Arctic Wolf™ Managed Risk basiert auf der branchenweit einzigen cloudnativen Plattform, die Security Operations als Concierge-Service anbietet. Damit können Unternehmen Netzwerke, Endpunkte und Cloudumgebungen fortlaufend scannen, um digitale Risiken zu quantifizieren. Der zuständige Sicherheitsberater vom Concierge Security® Team (CST) arbeitet direkt mit dem Kunden zusammen, um über einfache Schwachstellen hinausgehende Risiken zu ermitteln, den aktuellen Zustand der Umgebung zu bewerten und Risikomanagementprozesse zu implementieren, die den Sicherheitsstatus des Unternehmens im Laufe der Zeit verbessern.

Managed Cloud Monitoring

Mit dem Umstieg auf die Cloud müssen Unternehmen überall neue Herausforderungen in puncto Sicherheit meistern. Herkömmliche Sicherheitstools wie Firewalls, Advanced Endpoint Protection oder SIEM-Appliances bieten keinen wirksamen Schutz für Cloud-Workloads und Cloudanbieter übernehmen für viele wichtige Sicherheitsbereiche keine Haftung. Unternehmen haben massive Schwierigkeiten, ihre Teams mit Fachkräften zu besetzen, die auf das Thema Cybersicherheit in der Cloud spezialisiert sind. Und die Bedrohung für Cloudplattformen nimmt zu.

Arctic Wolf™ Managed Cloud Monitoring basiert auf der branchenweit einzigen cloudnativen Plattform, die Security Operations als Concierge-Service anbietet. Unternehmen, die sich hierfür entscheiden, können Sicherheitslücken und Angriffe in der Cloud direkt bei ihrem Eintreten erkennen – und zwar auf zahlreichen gängigen Plattformen. Der zuständige Sicherheitsberater aus dem Concierge Security® Team (CST) arbeitet direkt mit dem Kunden zusammen. Mit seiner Expertise zum Thema Cloudsicherheit steht er unterstützend bei der Implementierung, der Erkennung von Risiken und der laufenden Überwachung der Cloud bereit. Dies schafft die Basis, um die gewählte Cloudstrategie zu optimieren und dadurch den Sicherheitsstatus zu verbessern.

Anhang A: Total Economic Impact

Total Economic Impact ist eine von Forrester Research entwickelte Methodik, die die Entscheidungsfindungsprozesse eines Unternehmens zu technischen Fragen optimiert und Anbieter bei der Kommunikation des Leistungsversprechens ihrer Produkte und Dienstleistungen gegenüber Kunden unterstützt. Die TEI-Methodik erleichtert es Unternehmen, den messbaren Wert von IT-Initiativen gegenüber der oberen Führungsebene und anderen wichtigen geschäftlichen Stakeholdern zu demonstrieren, zu rechtfertigen und zu veranschaulichen.

Total Economic Impact – Ansatz

Nutzen ist der Wert, der dem Unternehmen durch das Produkt entsteht. Die TEI-Methodik gewichtet die Ermittlung des Nutzens und die Messung der Kosten gleichermaßen. Somit wird eine umfassende Untersuchung der Auswirkungen der Technologie auf das gesamte Unternehmen ermöglicht.

Kosten berücksichtigen alle Ausgaben, die zur Schaffung des beabsichtigten Mehrwerts oder Nutzens des Produkts erforderlich sind. Die Kostenkategorie innerhalb der TEI-Methodik erfasst die über die gegenwärtige Umgebung hinausgehenden Mehrkosten für die mit der Lösung verbundenen laufenden Kosten.

Flexibilität ist der strategische Wert, der bei zukünftigen Investitionen erzielt werden kann, sofern diese auf bereits getätigten Investitionen aufbauen. Die Möglichkeit, diesen Nutzen zu realisieren, stellt bereits einen Barwert dar, der prognostiziert werden kann.

Risiken messen die Unsicherheit der erhaltenen Nutzen- und Kostenprognosen: 1) die Wahrscheinlichkeit, dass die Prognosen den ursprünglichen Voraussagen entsprechen, und 2) die Wahrscheinlichkeit, dass die Prognosen über einen gewissen Zeitraum hinweg verfolgt werden. Risikofaktoren der TEI-Methodik basieren auf einer „Dreiecksverteilung“.

Die Spalte für die anfängliche Investition enthält Kosten, die zum „Zeitpunkt 0“ oder zu Beginn von Jahr 1 entstanden sind. Diese werden nicht reduziert. Alle anderen Cashflows werden unter Verwendung eines Rabatts am Ende des Jahres reduziert. Barwert- bzw. BW-Berechnungen werden für jede Gesamtkosten- und Nutzenschätzung vorgenommen. Kapitalwert- bzw. KW-Berechnungen in den Übersichtstabellen entsprechen der Summe der anfänglichen Investition und der diskontierten Cashflows für die einzelnen Jahre. Die Summen und Barwertberechnungen in den Tabellen für Gesamtnutzen, Gesamtkosten und Cashflow ergeben möglicherweise nicht den exakten Gesamtwert, da einige Beträge eventuell gerundet sind.

Barwert (BW)

Der Barwert oder aktuelle Wert der (diskontierten) Kosten- und Nutzenschätzungen zu einem gegebenen Zinssatz (dem Diskontsatz). Der Barwert für Kosten und Nutzen fließt in den Gesamtkapitalwert von Cashflows ein.

Kapitalwert (KW)

Der Barwert oder aktuelle Wert von (diskontierten) zukünftigen Netto-Cashflows zu einem gegebenen Zinssatz (dem Diskontsatz). Ein positiver Projektkapitalwert bedeutet normalerweise, dass die Investition vorgenommen werden sollte, sofern nicht andere Projekte höhere Kapitalwerte aufweisen.

Kapitalrendite

Die erwartete Rendite eines Projekts, angegeben als Prozentwert. Zur Berechnung des ROI wird der Nettonutzen (Nutzen abzgl. Kosten) durch die Kosten geteilt.

Diskontsatz

Der in der Cashflow-Analyse verwendete Zinssatz, mit dem der Zeitwert von Geld einbezogen wird. Unternehmen verwenden in der Regel Diskontsätze zwischen 8 % und 16 %.

Amortisierungszeitraum

Die Gewinnschwelle einer Investition. Dies ist der Zeitpunkt, an dem der Nettonutzen (Nutzen abzgl. Kosten) gleich der Anfangsinvestition bzw. den Eingangskosten ist.

FORRESTER®