DAS WICHTIGSTE FÜR EIN RENTABLES MANAGED-SECURITY-SERVICEGESCHÄFT

F-Secure

Der Markt für Firmencybersicherheit ist schnell gewachsen und wird voraussichtlich auch in den nächsten vier Jahren mit zweistelligen Wachstumsraten weiter zulegen.

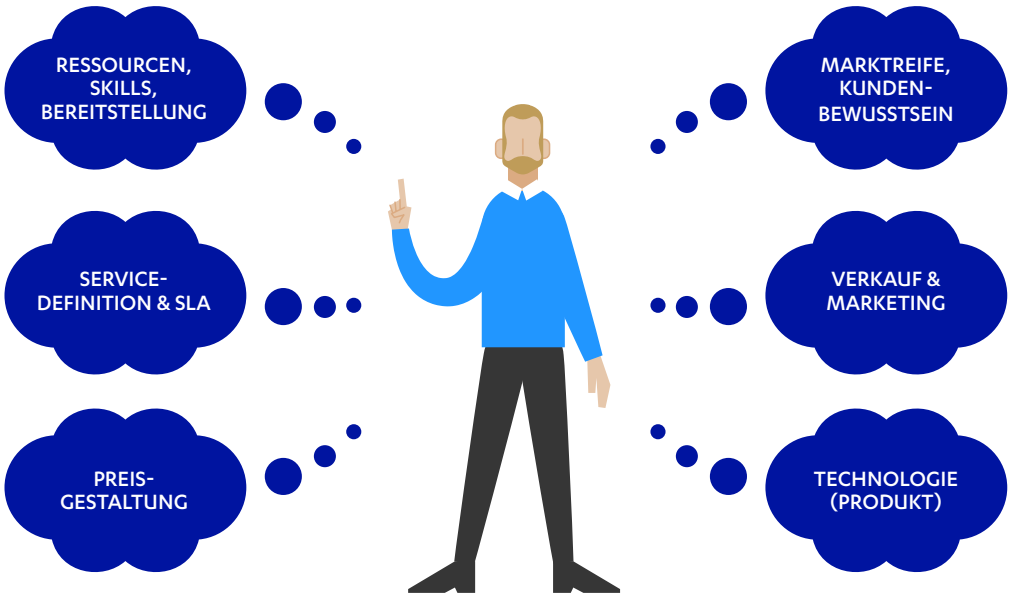
Gartner prognostiziert in seinem Marktreport von 2021[1] bei den Anwenderausgaben für Informationssicherheit eine konstante Wachstumsrate von über 10 % bis zum Jahr 2025, was insgesamt eine Marktgröße von rund 228 Mrd. US-Dollar ergibt.

Allerdings wachsen nicht alle Marktsegmente gleich stark, und es sind sicherlich nicht alle gleich profitabel. Ein anderer Gartner-Bericht[2] kann diese Ungleichheit sogar beziffern: „Die operativen Gewinnmargen bei allen Security-Segmenten lagen im Jahr 2019 zwischen –19 % und +23 %."

Wie sollten Managed Security Service Provider (MSSPs) also ihr Angebot gestalten? Die Auswahl der richtigen Dienste ist zweifellos eine Schlüsselkomponente, wenn es um größtmögliche Rentabilität geht. Es gilt jedoch noch eine ganze Reihe weiterer Dinge zu berücksichtigen.

In diesem Whitepaper zeigen wir die wichtigsten Komponenten auf, die ein rentables Managed-Security-Servicegeschäft ausmachen und auf Dauer sicherstellen. Wir stützen uns dabei auf unsere Erfahrung in der Zusammenarbeit mit den besten Managed-Security-Anbietern der Branche und mit unseren eigenen Managed Security Services.

MANAGED-SERVICE-ERWÄGUNGEN



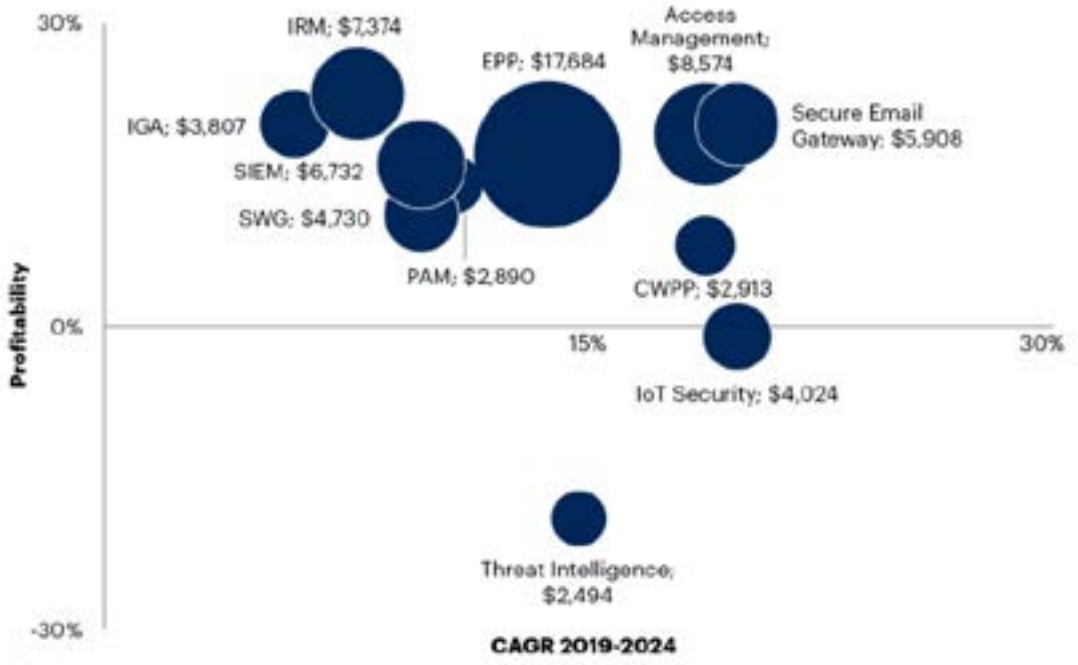
[1] Gartner: Forecast: Information Security and Risk Management, Worldwide 2019–2025. 2Q21 Update. 24. 06. 2021. ID G00752504.
[2] Gartner: Market Opportunity Map: Security and Risk Management Software, Worldwide. 10. 11. 2020. ID G00731517.

MARKTKENNTNIS

Das folgende Blasendiagramm stammt aus dem weltweiten Gartner-Report „Market Opportunity Map: Security and Risk Management Software“[2]. Es zeigt den Markt im Jahr 2024. Die Größe der Blasen entspricht den weltweiten Sicherheitsausgaben für das jeweilige Segment in Millionen Dollar. Die x-Achse verdeutlicht das Marktwachstum, gemessen als durchschnittliche jährliche Wachstumsrate (CAGR) von 2019 bis 2024. Die y-Achse stellt die von Gartner geschätzte operative Rentabilität in Prozent für 2019 dar.

Das sind nützliche Informationen für Sicherheitsanbieter, die überlegen, welche Dienste sie hinzunehmen wollen. Wir bei F-Secure meinen aber, dass es noch wichtiger ist, seinen lokalen Markt zu kennen – das zeigen die großen Unterschiede zwischen den einzelnen Segmenten.

MARKET OPPORTUNITY MAP FÜR SECURITY- UND RISIKOMANAGEMENT



Source: Gartner
Note: The bubble size represents 2024 worldwide security spending for each segment in millions of dollars.
CWPP = cloud workload protection platform; EPP = endpoint protection platform; IGA = identity governance and administration; IRM = integrated risk management; PAM = privileged account management; SIEM = security information and event management; SWG = secure web gateway
731517_C

Unserer Ansicht nach verdeutlichen diese Unterschiede auch, dass es beim Betrieb rentabler Services bestimmte Aspekte gibt, die über die einzelnen Segmente hinausgehen.

WAS MACHT EINEN PROFITABLEN MANAGED SECURITY SERVICE AUS?

F-Secure arbeitet mit über 1000 Partnern zusammen, und viele davon haben wir in den letzten Jahrzehnten beim Aufbau eines erfolgreichen Managed-Security-Servicegeschäfts unterstützt. Darüber hinaus betreiben wir mit dem Geschäftsbereich F-Secure Managed Detection & Response unseren eigenen Managed Security Service.

Jedes Unternehmen ist anders und steht vor eigenen Herausforderungen. Über die Jahre haben wir jedoch einige Merkmale festgestellt, die den erfolgreichsten und profitabelsten Unternehmen gemeinsam sind – und die wir auch in unser eigenes Betriebsmodell einbeziehen.

Diese Merkmale lassen sich grob in drei Kategorien einteilen: Menschen, Prozesse und Technologie. Natürlich gibt es so manche Überschneidungen, aber die Einteilung ist trotzdem ein guter Rahmen für die Darstellung der Ergebnisse aus unserer jahrzehntelangen Forschung.

MENSCHEN

Wir reden viel darüber, wie der technologische Fortschritt die Cybersecurity-Branche verändert, aber Tatsache bleibt: Wir sind weit davon entfernt, dass Technologie die notwendigen Investitionen in Personalentwicklung und Mitarbeiterbindung ersetzen könnte. Allerdings können erstklassige Technologie und die damit verbundene Unterstützung einen großen Beitrag dazu leisten, Ihr internes Fachwissen zu erweitern und auszubauen.

Cybersicherheitsexperten zu finden und zu halten, ist nach wie vor eine der größten Herausforderungen für Managed-Security-Anbieter. Letztlich sind es ja Ihre Mitarbeiter, die Ihr Produkt ausmachen. Hier sind unsere vier besten Tipps, wie Sie die besten Talente finden und halten.

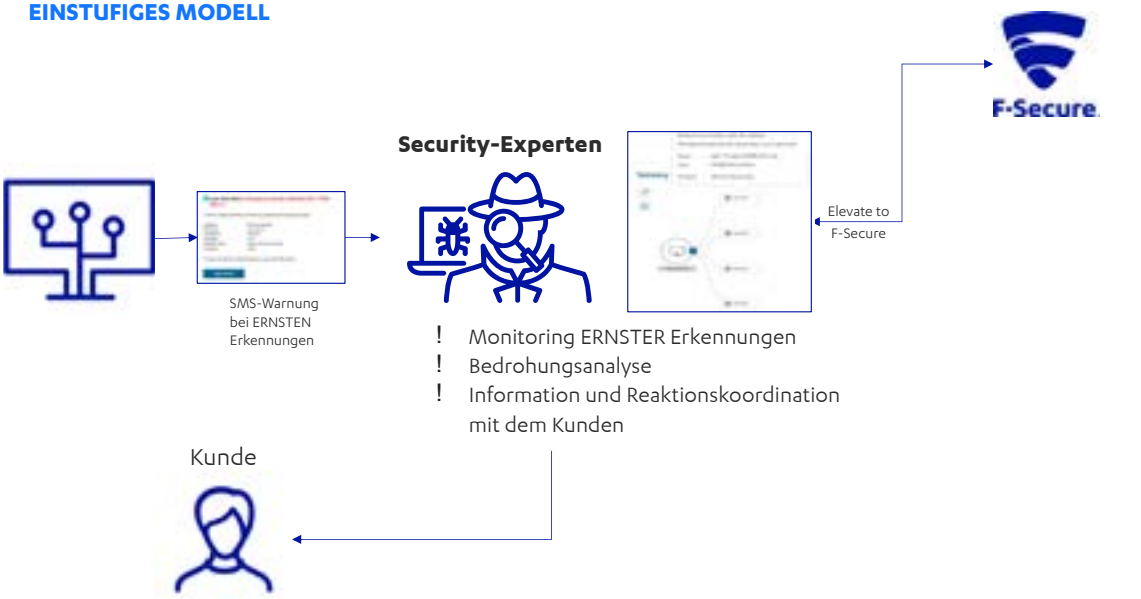
- **Sorgen Sie für eine nachhaltige Strategie bei Recruiting und Wachstum.** Natürlich ist es wichtig, jetzt die richtigen Talente zu finden, aber Sie müssen immer darauf gefasst sein, dass Mitarbeiter das Unternehmen verlassen und dass sich dies negativ auswirkt. Zu viel Personal schadet der Rentabilität, aber sobald Mitarbeiter ausscheiden, müssen Sie sie ersetzen, damit der Service nicht leidet. Wenn der Service leidet, leidet auch die Arbeitszufriedenheit der übrigen Beschäftigten, und am Ende stecken Sie in einem Teufelskreis.
- **Investieren Sie in die Personalentwicklung.** Die besten Anbieter von Cybersicherheitslösungen bieten umfangreiche Online- und Offline-Schulungen an. Machen Sie davon Gebrauch und nutzen Sie gegebenenfalls Co-Service-Modelle, um Ihre eigenen Kompetenzen zu ergänzen und zu erweitern!
- **Planen Sie Pausen und Recherchezeit ein.** Die Reaktion auf Bedrohungen kann eine anregende, erfüllende Arbeit sein, aber es lässt sich nicht leugnen, dass sie auch anstrengend ist und unter Umständen einen hohen Tribut von Ihren Mitarbeitern fordert. Bei F-Secure

arbeiten wir nach dem Prinzip „vier Tage arbeiten, vier Tage frei“, wobei zwei dieser vier Tage der Forschung dienen und nicht der unmittelbaren Abwehrarbeit. Unsere Threat Hunter sagen einstimmig, dass sie diese Forschungszeit am meisten schätzen.

- **Überlegen Sie genau, bevor Sie ein Stufensystem einführen.** Wir bei F-Secure haben nicht hierarchisch geregelt, wer worauf reagiert, und sehen abgestufte Systeme eher skeptisch. Natürlich haben wir Junior- und Senior-Mitglieder in den Teams, aber für uns funktioniert es besser, wenn alle Erfahrung mit allen Reaktionen sammeln können. Wenn Sie hingegen viele Anfragen niedriger Priorität haben, kann ein Stufensystem durchaus sinnvoll sein, sofern es sorgfältig umgesetzt wird, sodass es Alarmmüdigkeit und Burn-out vorbeugen kann.

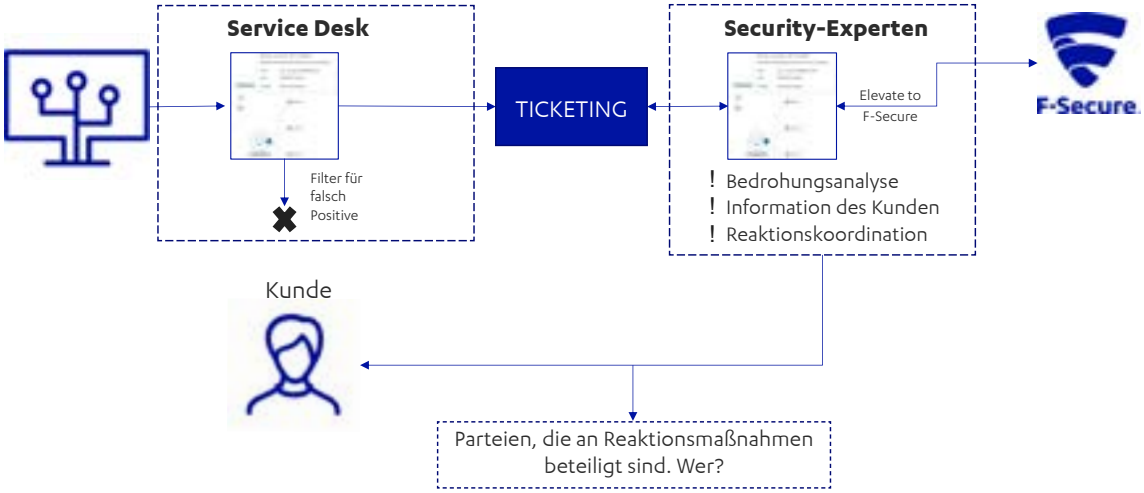
WIE FUNKTIONIERT DER SERVICE-PROZESS?

EINSTUFIGES MODELL



WIE FUNKTIONIERT DER SERVICE-PROZESS?

ZWEISTUFIGES MODELL



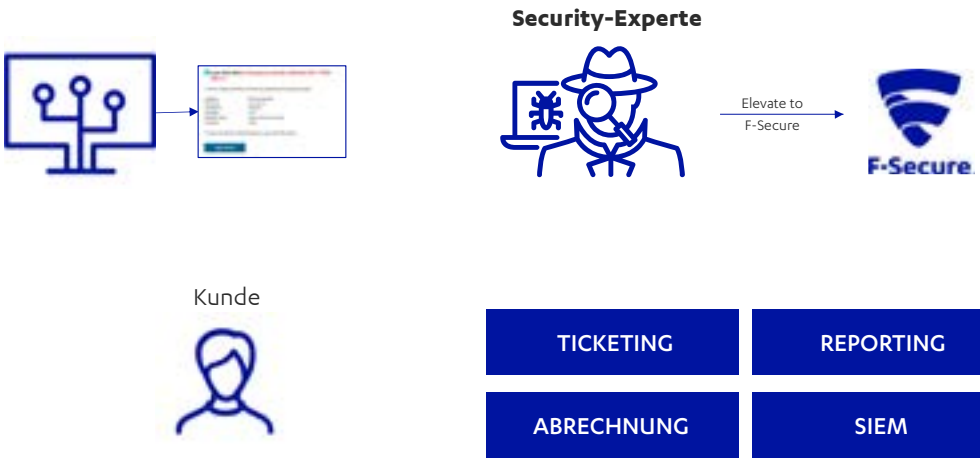
PROZESSE

Die richtigen Mitarbeiter zu finden, ist vielleicht der wichtigste Aspekt beim Aufbau eines rentablen Dienstes. Sind aber die Prozesse schlecht definiert, so verhindert das nicht nur, dass diese Mitarbeiter effektiv arbeiten können, sondern oft auch, dass sie sich überhaupt bewerben.

Im nächsten Abschnitt werden wir einige Prozessbeispiele aus der Praxis unserer Partner nennen. Hier sind schon einmal die wichtigsten Grundsätze, die Sie beherzigen sollten:

- **Sorgen Sie für Integration mit allen anderen Diensten, die sie anbieten.** Wenn Sie einen Security Service aufnehmen, dann ist das Wichtigste, dass er mit allen Ihren übrigen Diensten harmoniert, ob Sicherheitsdienste anderer Anbieter oder sonstige IT- bzw. Software-Services.
- **Definieren Sie Ihr SLA.** Ein SLA für die Geschäftszeiten (8/9/10–17) ist für viele Kunden vollkommen ausreichend, vielleicht ergänzt durch eine automatische Host-Isolierung bei ernsthaften Erkennungen. Ansonsten ist ein 24/7-Angebot dann sinnvoll, wenn Sie einen solches Service Level bereits für andere Dienste anbieten.
- **Planen Sie regelmäßige Berichte.** Reporting ist wichtig, weil Sie damit den Wert des Dienstes belegen. Auch wenn es nichts Größeres zu melden gibt, sollte der Kunde regelmäßig informiert werden oder Zugang zu einem Dashboard haben, das ihm zeigt, was der Dienst leistet.
- **Definieren und dokumentieren Sie alle Ihre Entscheidungen.** Unabhängig davon, wofür Sie sich entscheiden, sind wohl definierte und dokumentierte Prozesse zur Benachrichtigung des Kunden und die Bereitstellung von Anleitungen zur Problembehebung unerlässlich..

IHR PROZESSABLAUF



TECHNOLOGIE

Die dritte Säule eines rentablen Managed Security Services ist die Technologie. Wenn Sie die richtige Technologie wählen, können Sie die von Ihnen gewünschten Prozesse mit minimalem Aufwand für Ihre Mitarbeiter umsetzen.

Unserer Erfahrung nach sind dies die wichtigsten Punkte, die zu beachten sind, damit die von Ihnen gewählte Technologie Ihnen wirklich hilft, die betriebliche Effizienz und letztlich die Rentabilität zu maximieren:

1. **Produktqualität**

Es klingt wie eine Selbstverständlichkeit, aber wenn Sie wirklich erstklassige Lösungen verwenden, können Sie mithilfe von KI-Technologie das Rauschen ausfiltern und die Anzahl der Supportfälle reduzieren, was langfristig die betriebliche Effizienz und die Rentabilität steigert. Unabhängige Benchmarks wie AV TEST und Mitre-ATT&CK-Evaluierungen sind nützliche Quellen für den Anbietervergleich.

2. **Zentralisiertes Management**

Wir bei F-Secure sind der festen Überzeugung, dass die Zukunft der Cybersicherheit in All-in-one-Lösungen liegt. Das ist jedoch nicht die Realität der Gegenwart. Bis dahin ist es am besten, wenn Sie darauf achten, dass Sie all Ihre Lösungen in ein zentrales Management-system integrieren können. Wenn Analysten ihre Konzentration auf diverse Systeme aufteilen müssen, steigt das Risiko, dass sie etwas übersehen.

3. **Benutzeroberfläche**

Aus demselben Grund ist eine gute Benutzeroberfläche unerlässlich. Sie brauchen ein Produkt, das auf MSSP-Analysten als Hauptnutzer ausgerichtet ist. Ihre Service-Experten sollten auf einen Blick wissen, was zu tun ist und wo sie nachforschen müssen.

4. **Übergreifende Datennutzung**

Neben dem zentralen Management ist es wichtig, dass Sie sich für Technologie entscheiden, die mit Ihren anderen Lösungen spricht und Daten austauschen kann. Wenn Sie z. B. Lösungen für Endpunktschutz, Schwachstellenmanagement und E-Mail-Sicherheit unverbunden nebeneinander betreiben, entgeht Ihnen die Erkennungsleistung und die Effizienz, die sich aus der Kombination der erzeugten Daten ergibt.

5. **Lizenzoptionen**

Es hängt von den Volumen ab, die Sie verarbeiten, ob Sie mehr von den Fixkosten eines langfristigen Vertrags oder von der Flexibilität eines nutzungsbasierten Modells profitieren. Dies sollten Sie bei der Auswahl eines Anbieters unbedingt berücksichtigen.

WAS UND MIT WELCHEN RESSOURCEN?

Die Entscheidung darüber, welche Dienste Sie am besten anbieten und wie sie geleistet und mit Ressourcen ausgestattet werden sollten, ist natürlich etwas, das nur im Einzelfall zu klären ist. In unseren Servicedesign-Workshops denken wir diese Fragen mit unseren Partnern konkret durch. Aus dieser Erfahrung heraus können wir modellhaft einige Prozess und -Ressourcendesigns zeigen – auch wenn am Ende das, was am besten passt, sehr von der speziellen Situation abhängt.

Eine der ersten Fragen, die wir stellen, ist, wie weit der Service gehen soll. In der Regel bieten unsere Partner drei verschiedene Service Level an:

- **Technologiemanagement** – die Besorgung elementarer betrieblicher Aufgaben wie das Hinzufügen und Stilllegen von Geräten und die Installation von Updates.
- **Bedrohungsmonitoring** – die aktive Überwachung auf Bedrohungen und Schwachstellen sowie die Beratung des Kunden, wie diese zu beheben sind..
- **Aktive Reaktion und Behebung** – die Bereinigung von Schwachstellen und aktive Gegenmaßnahmen bei Bedrohungen.

Das reine Technologiemanagement bringt dem Kunden den geringsten Mehrwert und ist wohl das Geschäft mit der kleinsten Gewinnspanne. Die meisten unserer erfolgreichen Partner bieten daher irgendetwas zwischen Bedrohungsüberwachung und aktiver Reaktion an. Allerdings ist das Technologiemanagement oft der erste Schritt, den ein Kunde unternimmt, wenn er seine Sicherheit verbessern will, und kann insofern ein wichtiger Service im Portfolio sein.

Die Bedrohungsüberwachung lässt sich leichter als formalisierten Service anbieten, weil das Nutzenversprechen klar und der Umfang des Dienstes einfach zu definieren ist. Aktive Reaktion ist schwieriger zu bestimmen; das Serviceversprechen und die Beschreibung müssen hier ganz klar machen, welche Reaktionsfähigkeiten bzw. -aktionen der Service konkret umfasst.

Wir haben ein Modell entwickelt, mit dem wir unsere Partner bei der Kalkulation des Ressourcenbedarfs unterstützen können. Es berücksichtigt eine Reihe von Faktoren, z. B. das Service Level, die Anzahl der Erkennungen, die eine Vollzeitstelle pro Monat bearbeiten kann, und die durchschnittliche Anzahl der Erkennungen bei einer bestimmten Anzahl von Hosts. Wir sind gerne bereit, das im Einzelnen mit unseren Partnern durchzugehen.

WIR SIND HIER, UM ZU HELFEN

Die genannten Überlegungen sind nur einige der Dinge, die Sie beim Aufbau eines neuen Managed Security Services berücksichtigen sollten. Die gute Nachricht ist, dass Sie nicht auf sich allein gestellt sind. F-Secure hat jahrzehntelange Erfahrung in der Unterstützung seiner Partner und kann Ihnen mit Rat und Tat zur Seite stehen.

SERVICEDESIGN-WORKSHOPS

Mit den Servicedesign-Workshops helfen wir Partnern, die neue Dienste anbieten möchten, einen soliden Business Case aufzustellen. In den Workshops führen unsere Experten Sie durch die Schritte und Entscheidungen, die anstehen, wenn der Service rentabel werden soll.

Zu diesem Workshop gehört auch, dass wir unsere Partner mit unserem Business-Case-Rechner bekannt machen, der MSSPs dabei hilft, ihre Gewinnspanne für verschiedene Produkte und Dienste abzuschätzen und herauszufinden, ob ihr Volumen den Wechsel zu einer nutzungsbasierten Lizenz rechtfertigt.

Der Rechner berücksichtigt eine Reihe von Faktoren, darunter Technologiekosten, Personal- und Ausbildungskosten, Betriebskosten sowie sonstige Vertriebs- und Marketing-Kosten.

F-SECURE ELEMENTS

Damit unsere Partner möglichst frei in der Zusammenstellung von Security Services für ihre Kunden sind, haben wir bei F-Secure ein modulares, aber umfassendes Produktportfolio entwickelt, dessen einzelne Komponenten die komplette Sicherheitswertschöpfungskette abdecken und optimal miteinander integriert sind, vom Schwachstellenmanagement über den Endpunktschutz bis zu Erkennung und Reaktion. Managed Security Service Provider können damit flexible, abonnement- und nutzungsbasierte Cybersicherheitsdienste zusammenstellen. Das Management geschieht übersichtlich über eine einzige zentrale Konsole.

Zentrales Managementsystem

Wenn wir unsere Partner besuchen, stellten wir oft fest, dass die Analysten eine ganze Reihe von Browser-Fenstern geöffnet haben und sich Mühe geben, mit jedem davon ein anderes Produkt in einem anderen Managementsystem im Blick zu behalten. Uns war von Anfang an klar, dass so etwas nicht effizient sein kann. Also haben wir Elements entwickelt und damit alle unsere Lösungen in einem zentralen Managementsystem zusammengefasst.

Umfassende Sichtbarkeit

Auf diese Weise haben Ihre Analysten die Daten von Endpunktschutz, Schwachstellen-management und E-Mail-Schutz auf einem einzigen Bildschirm zusammengefasst. Das sorgt natürlich schlagartig für mehr Effizienz, wenn sich die Experten auf einen Punkt konzentrieren können. Darüber hinaus erhalten sie aber auch zusätzliche Einblicke und erkennen Zusammen-hänge, was bei den Silo-Lösungen zuvor gar nicht möglich gewesen wäre.

Schlanke Arbeitsabläufe

Das Maß an betrieblicher Effizienz, das Sie damit erreichen, ermöglicht ganz neue Arbeitsweisen und wird letztlich Ihre Personalkosten senken. Wir haben z. B. ausgerechnet, dass eine einfache Erkennung mit Elements mehr als zehnmal schneller geschieht als mit herkömmlichen Lösungen.

Elevate to F-Secure

Bei F-Secure arbeiten einige der besten Threat Hunter der Branche für unsere eigenen Managed Security Services. Mit Elevate to F-Secure stehen diese Spezialkenntnisse auch unseren Partnern zur Verfügung.

Sie haben dann nicht nur die Gewissheit, dass Sie die schwierigsten Fälle an unsere Elite-Cyber-experten eskalieren können, sondern können sich auch darauf verlassen, dass deren Fach-wissen Ihre internen Kapazitäten auf dem neuesten Stand hält und optimiert. Sie erhalten von uns einen umfassenden Vorfallbericht, sodass Sie Ihre eigenen Kompetenzen daran ausrichten können und gegen ähnliche Ereignisse in der Zukunft besser gewappnet sind.

NEUGIERIG GEWORDEN?

Wenn Sie mehr über das wissen wollen, was in diesem Whitepaper skizziert ist, nehmen Sie bitte Kontakt mit uns auf. Unsere Experten sprechen gerne mit Ihnen darüber, wie wir Sie beim Aufbau eines profitablen Managed-Security-Servicegeschäfts unterstützen können.

Email: vertrieb-de@f-secure.com
Telefon: +49 89 7874670
Web: https://www.f-secure.com/de/partners/business-products/managed-service-providers#become-a-partner

ÜBER F-SECURE

Niemand hat einen besseren Einblick in echte Cyberangriffe als F-Secure. Wir schließen die Lücke zwischen Erkennung und Reaktion. Zu diesem Zweck nutzen wir die unübertroffene Bedrohungsdatenerkennung von Hunderten der besten technischen Berater unserer Branche, aus Millionen von Geräten, die unsere preisgekrönte Software nutzen, sowie durch fortlaufende Innovationen im Bereich künstlicher Intelligenz. Führende Banken, Fluggesellschaften und Unternehmen vertrauen auf unser Engagement bei der Bekämpfung der gefährlichsten Bedrohungen der Welt.

Zusammen mit unserem Netzwerk an Top-Channel-Partnern und über 200 Serviceanbietern ist es unsere Mission, all unseren Kunden maßgeschneiderte unternehmensfähige Cybersicherheit zur Verfügung zu stellen. F-Secure wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd gelistet.

f-secure.com/business | twitter.com/fsecure | linkedin.com/company/f-secure-corporation

F-Secure