FORGENOVA

DER DEFINITIVE LEITFADEN FÜR MANAGED DETECTION AND RESPONSE

Cyber-Bedrohungen sind allgegenwärtig, und die Unternehmen in der Europäischen Union stehen vor besonderen Herausforderungen. Die Gewährleistung der Sicherheit der digitalen Ressourcen Ihres Unternehmens ist nicht verhandelbar.

Dieser Leitfaden ist Ihr Wegweiser, um die Komplexität der Cybersicherheit zu bewältigen und Ihre wertvollen Unternehmungen mit MDR zu schützen.

TABLE OF CONTENTS

Was ist MDR im Kern? 01

Vereinfachung der Cybersicherheit für Ihre Branche 02

Navigieren im medizinischen Grenzbereich 02

Widerstandsfähigkeit der Produktion 02

Sicherung der finanziellen Grundlagen 02

Stärkung des Energie-Ökosystems 03

Aufbau einer sicheren Zukunft 03

Bewältigung der Herausforderungen in Bezug auf Personal und Fachwissen 04

Geben Sie MDR ein 04

Wachsamkeit rund um die Uhr 04

Proaktive Erkennung von Bedrohungen 04

Schnelle Reaktion auf Vorfälle 04

Ein Team, das Ihre Branche versteht 05

Maßgeschneiderte Verteidigung 05

Ressourcen freisetzen 05

Zähmung der Komplexität der Cybersicherheit 06

Das Labyrinth der Komplexität 06

Entwirren Sie sich mit dem MDR 06

Abwehr von Ransomware und Cyberangriffen 08

Die Bedrohung durch Ransomware 08

Die proaktive Haltung des MDR 09

Der wirtschaftliche Vorteil: 10

MDR als kosteneffiziente Lösung

Compliance leicht gemacht: 11

Die Nutzung von MDR zur Erfüllung gesetzlicher Anforderungen

Erfolgsgeschichten aus der Praxis: 12

Fallstudien über die Auswirkungen des MDR auf Unternehmen wie das Ihrige

Auswahl des MDR-Anbieters 14

Verstehen Sie Ihre Bedürfnisse 14

Schlüsselfaktoren für die Auswahl eines MDR-Anbieters 14

Bewerten Sie 15

Eine Entscheidung treffen 16

Was ist MDR im Kern?

Managed Detection and Response (MDR) ist ein Cybersicherheitsdienst, der Unternehmen eine Rund-um-die -Uhr-Überwachung und Bedrohungserkennung für ihre IT-Infrastruktur bietet. Dies kann Unternehmen dabei helfen, Sicherheitsbedrohungen schnell und effektiv zu erkennen und darauf zu reagieren, was für den Schutz ihrer Daten und Vermögenswerte unerlässlich ist.

MDR ist wie ein Team von Sicherheitsexperten, das rund um die Uhr auf Abruf zur Verfügung steht und die IT-Systeme Ihres Unternehmens auf Anzeichen von Problemen überwacht. Sie setzen eine Vielzahl von Tools und Techniken ein, um Ihre Systeme auf verdächtige Aktivitäten zu überwachen, und sie können alle Bedrohungen, die sie finden, schnell untersuchen und darauf reagieren.

MDR kann für Unternehmen jeder Größe eine gute Möglichkeit sein, ihre Cybersicherheit zu verbessern. Es kann Unternehmen helfen,:

- **Reduzieren Sie das Risiko von Datenschutzverletzungen**
- **Verbesserung der Reaktionszeit auf Vorfälle**
- **Erfüllung gesetzlicher Anforderungen**
- **Sparen Sie Geld bei den Sicherheitskosten**

Vereinfachung der Cybersicherheit für Ihre Branche

Navigieren im medizinischen Grenzbereich

Im Bereich des Gesundheitswesens, in dem die Unantastbarkeit von Patientendaten an erster Stelle steht, ist die digitale Domäne ein zweischneidiges Schwert. Auf der einen Seite beschleunigt sie medizinische Durchbrüche, auf der anderen Seite setzt sie sensible Informationen böswilligen Akteuren aus. MDR übernimmt die Rolle des Wächters und schützt die Vertraulichkeit von Patientendaten durch Erkennung von Bedrohungen in Echtzeit, verstärkte Compliance-Maßnahmen und schnelle Reaktion auf Vorfälle. Mit MDR bleibt Ihr Fokus dort, wo er sein sollte - auf der Bereitstellung einer hervorragenden Patientenversorgung.

Widerstandsfähigkeit der Produktion

Das verarbeitende Gewerbe ist der Herzschlag des industriellen Fortschritts. Dieser Fortschritt ist jedoch auch eine Zielscheibe, da Cyberkriminelle versuchen, Schwachstellen in vernetzten Systemen auszunutzen. MDR stärkt Ihre Produktionsabläufe durch ständige Überwachung und sorgt dafür, dass die Fließbänder ungehindert weiterlaufen, während jeder Versuch, Ihre Produktionsprozesse zu stören, vereitelt wird.

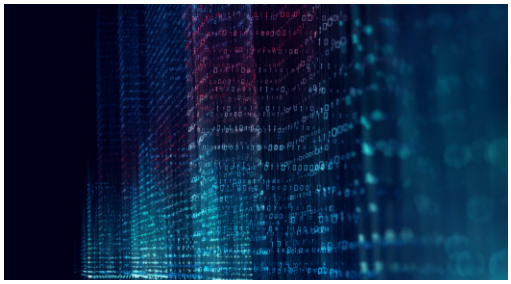
Sicherung der finanziellen Grundlagen

Der Finanzsektor lebt vom Vertrauen und macht die Cybersicherheit zu einem nicht verhandelbaren Eckpfeiler. MDR wird zu Ihrem finanziellen Wächter, wachsam gegen betrügerische Aktivitäten, Datenverletzungen und Ransomware-Versuche. Er sorgt dafür, dass Ihre Transaktionen sicher bleiben, das Vertrauen Ihrer Kunden unerschüttert bleibt und Ihr Finanzsystem angesichts der sich entwickelnden Bedrohungen widerstandsfähig ist.

Stärkung des Energie-Ökosystems

Der Energiesektor treibt den Fortschritt voran, aber er zieht auch die Aufmerksamkeit derjenigen auf sich, die versuchen, Schwachstellen in kritischen Infrastrukturen auszunutzen. MDR ist Ihr digitales Schutzschild, das die Integrität Ihrer Energiesysteme bewahrt, Cyberangriffe abwehrt, die die Stromverteilung stören könnten, und einen nahtlosen Energiefluss zur Förderung des Wohlstands gewährleistet.

Aufbau einer sicheren Zukunft



In der Baubranche, in der sich Baupläne von Papier zu Pixeln entwickeln, birgt die Konvergenz von digitaler und physischer Welt einzigartige Risiken. MDR schützt Ihre architektonischen Entwürfe, Projektzeitpläne und Ihr wertvolles geistiges Eigentum. Er sorgt dafür, dass Ihr digitaler Fußabdruck belastbar bleibt, um Ihren Wettbewerbsvorteil zu bewahren und Ihnen eine sichere Zukunft zu ermöglichen.

Bewältigung der Herausforderungen in Bezug auf Personal und Fachwissen

Der Mangel an Fachkräften im Bereich der Cybersicherheit stellt für Unternehmen in ganz Europa eine große Herausforderung dar. Da sich die Cyber-Bedrohungslandschaft weiterentwickelt, wird es zu einem schwierigen Unterfangen, qualifizierte Fachkräfte zu finden und zu halten, um Ihre digitalen Werte zu schützen.

Geben Sie MDR ein

MDR ist nicht nur eine Technologie, sondern ein Team erfahrener Cybersicherheitsexperten, die gemeinsam daran arbeiten, Ihr Unternehmen zu schützen. Mit MDR erhalten Sie Zugang zu einer engagierten Gruppe von Experten, die über die neuesten Kenntnisse, Taktiken und Technologien verfügen.

Wachsamkeit rund um die Uhr

MDR hält sich nicht an die üblichen Geschäftszeiten, wenn es darum geht, Ihre digitale Festung zu schützen. Da Cyber-Bedrohungen jederzeit auftreten können, ist MDR rund um die Uhr wachsam. Diese ununterbrochene Überwachung stellt sicher, dass potenzielle Bedrohungen sofort erkannt und angegangen werden, egal ob sie mitten in der Nacht oder während der geschäftigsten Stunden Ihres Betriebs auftauchen.

Proaktive Erkennung von Bedrohungen

MDR setzt modernste Tools ein, um den Netzwerkverkehr zu überwachen, Datenmuster zu analysieren und kleinste Abweichungen zu erkennen. Dieser proaktive Ansatz gewährleistet, dass potenzielle Bedrohungen erkannt werden, bevor sie Schaden anrichten.

Schnelle Reaktion auf Vorfälle

Zeit wird zu Ihrer wertvollsten Ressource, wenn eine Cyber-Bedrohung Ihre digitalen Schutzmaßnahmen durchbricht. Hier kommen die schnellen Reaktionsmöglichkeiten von MDR ins Spiel. Wie ein Feuerwehrmann, der sich beeilt, ein Feuer zu löschen, treten die Experten von MDR beim ersten Anzeichen von Problemen schnell in Aktion. Sie beurteilen die Situation, neutralisieren die Bedrohung und setzen Gegenmaßnahmen ein, um den Schaden zu minimieren. Dieser proaktive Ansatz stellt sicher, dass Cybervorfälle eingedämmt werden, bevor sie eskalieren, und verhindert so weitreichende Störungen und mögliche Datenschutzverletzungen.

Ein Team, das Ihre Branche versteht

MDR-Anbieter verstehen die Feinheiten Ihrer spezifischen Branche und passen ihre Strategien an Ihre Herausforderungen und Compliance-Anforderungen an.

Maßgeschneiderte Verteidigung

Die MDR geht über einen Einheitsansatz hinaus. Er erkennt an, dass jede Branche in einem einzigartigen Ökosystem mit eigenen Herausforderungen, Vorschriften und Schwachstellen arbeitet. Ganz gleich, ob Sie im Gesundheitswesen, in der Fertigung, im Finanzwesen, im Energiesektor oder im Baugewerbe tätig sind, MDR-Anbieter kennen die Feinheiten Ihres Sektors. Dieses branchenspezifische Fachwissen ermöglicht es ihnen, ihre Strategien und Techniken so zu gestalten, dass sie nahtlos auf die Bedürfnisse Ihres Unternehmens abgestimmt sind.

Ressourcen freisetzen

Durch die Zusammenarbeit mit einem MDR-Anbieter erschließen Sie sich einen Fundus an Fachwissen, der andernfalls aufgrund von Budgetbeschränkungen oder des Mangels an qualifizierten Fachkräften nicht zur Verfügung gestanden hätte.

MDR verwandelt das Bild der Cybersicherheit von einer Unsicherheit in ein Bild der Befähigung. Es geht nicht nur darum, Lücken in Ihrem Fachwissen zu schließen - es geht darum, ein erfahrenes Team zu haben, das Ihnen im Angesicht von Cyberangreifern den Rücken freihält.

Zähmung der Komplexität der Cybersicherheit

Die Komplexität der Cybersicherheit wirkt oft wie ein furchterregender Widersacher. Die Navigation durch eine Landschaft voller sich ständig weiterentwickelnder Bedrohungen, komplizierter Technologien und der Notwendigkeit ständiger Wachsamkeit kann selbst die sorgfältigsten Organisationen überfordern.

Das Labyrinth der Komplexität

Sich in der Cybersicherheitslandschaft zurechtzufinden, kann sich oft wie eine Reise durch ein verwirrendes Labyrinth anfühlen. Die miteinander vernetzten Wege der Technologie, die versteckten Korridore potenzieller Schwachstellen und die drohenden Schatten von Cyber-Bedrohungen bilden ein komplexes Labyrinth, dessen Navigation Fachwissen erfordert.

Entwirren Sie sich mit dem MDR

Managed Detection and Response (MDR) wird zu Ihrem Wegweiser in diesem komplizierten Labyrinth. MDR wirkt wie ein Leuchtfeuer der Klarheit, das den Weg durch das Labyrinth erhellt, indem es die komplizierten Fäden der Komplexität entwirrt. Mit MDR als Ihrem treuen Begleiter verwandelt sich das Labyrinth in eine überschaubare Reise, die es Ihnen ermöglicht, sich auf Ihre Geschäftsziele zu konzentrieren, ohne von der Komplexität der Cybersicherheit überwältigt zu werden.

- **Navigieren durch die Flut von Warnmeldungen**

Der unaufhaltsame Strom von Warnmeldungen kann einer sintflutartigen Überschwemmung gleichen. MDR nutzt die Leistung fortschrittlicher Analysen und maschinellen Lernens, um eine intelligente Triage vorzunehmen und echte Bedrohungen zu erkennen, während falsch positive Meldungen herausgefiltert werden. Dieser ausgeklügelte Sortierprozess stellt sicher, dass Ihr Team seine Aufmerksamkeit genau dorthin lenkt, wo sie gebraucht wird.

• Einheitliche Bedrohungsdaten

MDR bietet einen umfassenden Überblick über potenzielle Risiken, indem Bedrohungsdaten aus der gesamten digitalen Landschaft zusammengeführt werden. So kann Ihr Unternehmen Bedrohungen proaktiv angehen, bevor sie sich manifestieren, und den Spieß umdrehen.

• Zentralisiertes Vorfallmanagement

MDR richtet einen zentralen Knotenpunkt ein, an dem Vorfälle verwaltet, nachverfolgt und bearbeitet werden. Dieser rationalisierte Ansatz beseitigt die Verwirrung, die durch verstreute Warnungen entsteht, und stellt sicher, dass jede potenzielle Bedrohung sorgfältig überwacht wird und darauf reagiert werden kann.

• Vereinfachte Einhaltung von Vorschriften

Mit der Unterstützung von MDR wird das Navigieren durch die komplexe Landschaft der Einhaltung von Vorschriften vereinfacht. MDR unterstützt Ihr Unternehmen bei der Einhaltung relevanter Standards und Vorschriften und reduziert so die Belastung durch komplexe Compliance-Probleme.

• Nahtlose Technologie-Integration

MDR lässt sich nahtlos in Ihre bestehende Technologieinfrastruktur integrieren, schließt Lücken und optimiert Ihre Cybersicherheitsbemühungen. Diese Integration ermöglicht es Ihnen, Ihre aktuellen Investitionen zu nutzen und gleichzeitig Ihre gesamte Verteidigungsstrategie zu verbessern.

ANGEBOT ERHALTEN

Abwehr von Ransomware und Cyberangriffen

Die Bedrohung durch Ransomware und Cyberangriffe ist größer denn je. Die Aussicht, dass wertvolle Daten als Geiseln gehalten werden, der Betrieb gestört wird und die Struktur Ihres Unternehmens gefährdet ist, ist eine beängstigende Realität.

Die Bedrohung durch Ransomware

Die Zahl der Ransomware-Angriffe ist im Jahr 2021 um 150 % gestiegen. Dies ist ein deutlicher Anstieg gegenüber dem Vorjahr, und dieser Trend wird sich voraussichtlich auch 2023 fortsetzen.

Ransomware-Angriffe zielen mittlerweile auf Unternehmen aller Größenordnungen ab, auch auf kleine Unternehmen.

In der Vergangenheit waren Ransomware-Angriffe vor allem auf große Unternehmen ausgerichtet. In den letzten Jahren sind Ransomware-Angriffe jedoch immer raffinierter geworden und zielen nun auf Unternehmen aller Größenordnungen ab.

Die Wahrscheinlichkeit, dass Ransomware-Angriffe erfolgreich sind, ist gestiegen.

In der Vergangenheit konnten viele Unternehmen ihre Daten nach einem Ransomware-Angriff aus Backups wiederherstellen. In den letzten Jahren sind Ransomware-Angriffe jedoch immer raffinierter geworden und verschlüsseln nun eher Daten, die nicht aus Backups wiederhergestellt werden können.

Ransomware-Angriffe haben inzwischen erhebliche Auswirkungen auf die Weltwirtschaft.

Im Jahr 2021 kosteten Ransomware-Angriffe Unternehmen schätzungsweise 20 Milliarden US-Dollar. Das ist eine beträchtliche Summe, und dieser Trend wird sich voraussichtlich bis 2023 fortsetzen.

Die proaktive Haltung des MDR

MDR erweist sich als standhafter Verteidiger gegen die Bedrohung durch Ransomware. Er wartet nicht darauf, dass Ransomware zuschlägt, sondern sucht proaktiv nach Anzeichen für eine Gefährdung und nach Verhaltensmustern, die auf Ransomware-Aktivitäten hindeuten. Indem MDR diese Bedrohungen bereits im Anfangsstadium identifiziert, verhindert es, dass Ransomware in Ihren Systemen Fuß fasst.

Abwendung der Katastrophe

MDR fungiert als Ihr digitales Schutzschild, das Cyberangriffe abfängt und abwehrt, bevor sie Ihren Schutz durchbrechen können. Diese proaktive Haltung stellt sicher, dass Ihr Unternehmen auch im Angesicht entschlossener Angreifer widerstandsfähig und einsatzfähig bleibt.

Schutz vor Zero-Day-Schwachstellen

MDR ist mit den neuesten Bedrohungsdaten ausgestattet, die es ihm ermöglichen, Zero-Day-Schwachstellen zu erkennen und zu bekämpfen - also solche, die bisher unbekannte Schwachstellen ausnutzen.

Schnelle Erholung

Im Falle eines Angriffs ermöglicht die schnelle Reaktion von MDR eine rasche Wiederherstellung. So wird Ihr Unternehmen stärker und widerstandsfähiger und ist besser auf künftige Herausforderungen vorbereitet.

Wahrung der Geschäftskontinuität

Die wachsame Haltung von MDR stellt sicher, dass Ihr Geschäftsbetrieb ohne Unterbrechung weiterläuft. Durch die Vereitelung von Cyberangriffen und die Neutralisierung von Bedrohungen schützt MDR Ihre Einnahmequellen, das Vertrauen Ihrer Kunden und den Ruf Ihrer Marke.

Der wirtschaftliche Vorteil: MDR als kosteneffiziente Lösung

MDR bietet eine kosteneffiziente Lösung, die Ihnen die finanzielle Belastung durch die Einstellung von eigenem Personal, kontinuierliche Schulungen und die Auseinandersetzung mit steigenden Kosten erspart.

Balance zwischen Sicherheit und Budget

Die komplexe Gleichung der Cybersicherheit erfordert einen Balanceakt zwischen luftdichtem Schutz und finanzieller Umsicht. MDR bietet eine Lösung, die beide Elemente miteinander in Einklang bringt und es Ihnen ermöglicht, eine beeindruckende Sicherheit zu erreichen, ohne Ihr Budget zu strapazieren.

MDR: Eine finanziell kluge Entscheidung

Wenn Sie sich für MDR entscheiden, treffen Sie eine finanziell kluge Entscheidung. Herkömmliche Ansätze für die Cybersicherheit beinhalten die Einstellung, Schulung und Beibehaltung eines internen Teams, was sowohl zeitaufwändig als auch kostspielig sein kann. MDR hingegen bietet eine kostengünstige Alternative, die Ihnen diese ressourcenintensiven Bemühungen erspart.

Einsparungen über die Gehälter hinaus

Die mit MDR verbundenen Kosteneinsparungen gehen weit über die Gehälter hinaus. Wenn Sie interne Cybersicherheitsexperten einstellen, tragen Sie nicht nur die Kosten für deren Vergütung, sondern auch die Gemeinkosten, die mit Vollzeitbeschäftigten verbunden sind. Zu diesen Gemeinkosten gehören Sozialleistungen, Arbeitsplatz, Ausrüstung und fortlaufende Schulungen, um mit der sich weiterentwickelnden Bedrohungslandschaft Schritt zu halten.

Eine Investition in Werte

Wenn Sie sich für MDR entscheiden, sparen Sie nicht nur Kosten, sondern Sie investieren auch in Werte. Das Geld, das Sie durch die Vermeidung von Gemeinkosten einsparen, kann in strategische Initiativen fließen, die das Unternehmenswachstum und die Innovation fördern. Diese Umleitung von Ressourcen ermöglicht es Ihnen, Budgetentscheidungen zu treffen, die mit den übergeordneten Zielen Ihres Unternehmens übereinstimmen.

Vorhersehbare Budgetierung

Einer der bemerkenswerten Vorteile von MDR ist die vorhersehbare Budgetierung. Bei internem Personal können die Ausgaben aufgrund von Faktoren wie Mitarbeiterfluktuation, Schulungskosten und unerwarteten Ausfallzeiten aufgrund von Personalengpässen unvorhersehbar sein. MDR bietet einen stabilen finanziellen Rahmen, so dass Sie Ihre Ressourcen strategischer einsetzen können.

Fachwissen ohne Overhead

MDR bietet Ihnen Zugang zu einem Team von Cybersicherheitsexperten, ohne dass die mit einem eigenen Team verbundenen erheblichen Gemeinkosten anfallen. Sie profitieren von deren Fachwissen und Spezialkenntnissen und vermeiden gleichzeitig die finanzielle Belastung, die oft mit der Unterhaltung eines internen Teams einhergeht.

MDR ist nicht nur eine Sicherheitsmaßnahme, sondern auch eine fiskalisch verantwortungsvolle Entscheidung, die es Ihrem Unternehmen ermöglicht, sich in der digitalen Landschaft sicher zu bewegen.

Holen Sie sich ein Angebot und sehen Sie, wie viel Sie sparen können

GET YOUR FREE QUOTE

Compliance leicht gemacht: Die Nutzung von MDR zur Erfüllung gesetzlicher Anforderungen

- Unternehmen jeder Größe stehen zunehmend unter dem Druck, eine Vielzahl von Vorschriften wie NIS2, HIPAA und ISO 27001 einzuhalten.
- Dies gilt insbesondere in Europa, wo es eine Reihe strenger Vorschriften für Datenschutz, Privatsphäre und Cybersicherheit gibt.
- Eine Möglichkeit für Unternehmen, die Einhaltung dieser Vorschriften zu gewährleisten, ist die Implementierung einer Managed Detection and Response (MDR)-Lösung. MDR ist ein Dienst, der Unternehmen eine 24/7-Überwachung und Bedrohungserkennung für ihre IT-Infrastruktur bietet. Dies kann Unternehmen dabei helfen, Sicherheitsbedrohungen schnell und effektiv zu erkennen und darauf zu reagieren, was für die Einhaltung von Vorschriften unerlässlich ist.
- MDR kann Unternehmen auch dabei helfen, Nachweise für die Einhaltung von Vorschriften zu sammeln. Dies kann wichtig sein, wenn ein Unternehmen jemals von einer Aufsichtsbehörde geprüft wird.

Im Folgenden sind einige Möglichkeiten aufgeführt, wie MDR den Nachweis der Einhaltung der Vorschriften erbringen kann:

Audit-Protokolle

MDR-Lösungen erfassen in der Regel detaillierte Prüfprotokolle aller Aktivitäten in der IT-Infrastruktur eines Unternehmens. Diese Protokolle können als Nachweis für die Einhaltung von Vorschriften verwendet werden, die von Unternehmen verlangen, ihre Sicherheitskontrollen und -verfahren zu dokumentieren.

Bedrohungsdaten

MDR-Lösungen sammeln auch Bedrohungsdaten aus einer Vielzahl von Quellen. Diese Daten können verwendet werden, um Sicherheitsbedrohungen zu identifizieren und auf sie zu reagieren, die für die spezifische Branche und den Standort eines Unternehmens relevant sind. Diese Informationen können auch verwendet werden, um gegenüber einer Aufsichtsbehörde nachzuweisen, dass ein Unternehmen Maßnahmen zum Schutz seiner IT-Infrastruktur vor bekannten Bedrohungen ergreift.

Berichte zur Reaktion auf Vorfälle

MDR-Lösungen erstellen in der Regel Berichte über die Reaktion auf Vorfälle, in denen die Schritte dokumentiert werden, die zur Untersuchung und Reaktion auf Sicherheitsvorfälle unternommen wurden. Diese Berichte können verwendet werden, um gegenüber einer Aufsichtsbehörde nachzuweisen, dass ein Unternehmen über ein Verfahren zur rechtzeitigen und wirksamen Reaktion auf Sicherheitsvorfälle verfügt.

Wir bieten ein Webinar an, in dem die Anforderungen der NIS2-Konformität ausführlicher behandelt werden

Aufzeichnung ansehen

Erfolgsgeschichten aus der Praxis: Fallstudien über die Auswirkungen des MDR auf Unternehmen wie das Ihrige

Unternehmen, unabhängig von ihrer Branche, müssen sich in der sich ständig verändernden Bedrohungslandschaft zurechtfinden und gleichzeitig das Vertrauen der Kunden, die Einhaltung von Vorschriften und die betriebliche Effizienz aufrechterhalten. Im Folgenden finden Sie einige Erfolgsgeschichten aus der Praxis, die die Leistungsfähigkeit der Managed Detection and Response (MDR)-Lösungen von ForeNova verdeutlichen.

Schutz der Geschäftsintegrität bei der CPS GmbH Die

Vertrauen in den Schutzschild bei einer führenden Zeitung

Mehr Sicherheit im Gesundheitswesen bei ChipSoft

Umsetzung von Vorschriften in einem großen Krankenhaus

Schutz der Geschäftsintegrität bei der CPS GmbH Die

CPS GmbH, ein weltweit tätiger Spezialdistributor, stand vor einer echten Herausforderung: eine wachsende Bedrohungslandschaft und der Bedarf an erhöhter Sicherheitstransparenz. NovaCommand, die MDR-Lösung von ForeNova, erwies sich als entschlossener Partner.

Durch die Überwachung des gesamten Netzwerkverkehrs und die auf KI und maschinellem Lernen basierende Verhaltensanalyse gewährleistet NovaCommand eine frühzeitige Erkennung und Intervention von Bedrohungen. Für die CPS GmbH war NovaCommand nicht nur eine Sicherheitslösung, sondern ein Weg, sich auf das Geschäft zu konzentrieren, in der Gewissheit, dass ihr Netzwerk gegen Cyber-Bedrohungen geschützt ist.

Vertrauen in den Schutzschild bei einer führenden Zeitung

Eine bekannte Nachrichtenpublikation stand vor der schwierigen Aufgabe, Nachrichten zu liefern und gleichzeitig sensible Informationen zu schützen. NovaMDR spielte eine entscheidende Rolle bei der Stärkung ihrer Cybersicherheitsstrategie. Diese Fallstudie zeigt, wie NovaMDRs Kombination aus modernster Technologie und menschlicher Expertise gutartige und bösartige Bot-Aktivitäten herausfiltert und die Datenintegrität bewahrt. Mit einem proaktiven Ansatz für das Incident Management wurde die Cybersicherheit der Publikation gestärkt und sowohl ihr Ruf als auch das Vertrauen ihrer Leser geschützt.

Mehr Sicherheit im Gesundheitswesen bei ChipSoft

Im Gesundheitswesen sind die Sicherung von Patientendaten und die Aufrechterhaltung von Abläufen von größter Bedeutung. ChipSoft, ein führender Anbieter von elektronischen Gesundheitsakten (EHR), wandte sich an NovaMDR, um die Herausforderungen in den Bereichen Sicherheit, Compliance und Effizienz zu meistern. NovaMDRs Fähigkeiten bei der Überwachung aller Netzwerk- und Endpunktaktivitäten in Verbindung mit seiner KI-gestützten Bedrohungserkennung stellten die Integrität der medizinischen Daten sicher. Durch die Vereinfachung der Compliance und die Verbesserung der Sicherheit ermöglichte NovaMDR ChipSoft, sich auf seine Kernaufgabe zu konzentrieren: die Bereitstellung herausragender medizinischer Dienstleistungen bei gleichzeitiger Gewährleistung des Schutzes der Patientendaten.

Umsetzung von Vorschriften in einem großen Krankenhaus

Krankenhäuser, ein Hauptziel für Cyberangriffe, müssen strenge Vorschriften erfüllen, ohne die Patientenversorgung zu gefährden. Diese Fallstudie zeigt, wie NovaMDR es einem großen Krankenhaus ermöglichte, sich schnell an neue Sicherheitsvorschriften anzupassen. Die Flexibilität von NovaMDR, die Asset-Management-Funktionen und die agentenlose Architektur ermöglichten eine umfassende Netzwerktransparenz. Durch die Zusammenarbeit mit dem SOC von ForeNova sicherte sich das Krankenhaus eine 24/7-Überwachungslösung, die komplexe Benutzerszenarien beherrscht und die Einhaltung der sich entwickelnden Vorschriften gewährleistet.

Mit NovaMDR können Sie Ihr Unternehmen schützen, das Vertrauen Ihrer Kunden bewahren und in einer digitalen Welt voller Herausforderungen mit Zuversicht voranschreiten.

Keine Verpflichtungen.
Keine Kreditkarte erforderlich.

Auswahl des MDR-Anbieters

Die Auswahl des richtigen MDR-Anbieters (Managed Detection and Response) ist eine wichtige Entscheidung, die die Cybersicherheitslage Ihres Unternehmens beeinflussen kann.

Verstehen Sie Ihre Bedürfnisses

Bevor Sie mit dem Auswahlprozess beginnen, müssen Sie die besonderen Anforderungen und Herausforderungen Ihrer Organisation im Bereich der Cybersicherheit verstehen. Evaluieren Sie Ihre aktuelle Sicherheitsinfrastruktur, Probleme, Compliance-Anforderungen und Geschäftsziele.

Schlüsselfaktoren für die Auswahl eines MDR-Anbieters

01

Kompetenz und Erfahrung

Suchen Sie nach einem Anbieter mit einer nachgewiesenen Erfolgsbilanz in der Cybersicherheitsbranche. Prüfen Sie die Erfahrung des Anbieters bei der Bewältigung von Vorfällen, der Eindämmung von Bedrohungen und der Anpassung an die sich entwickelnde Bedrohungslandschaft.

02

Fortschrittliche Technologie

Stellen Sie sicher, dass der Anbieter modernste Technologien einsetzt, einschließlich KI, maschinelles Lernen und Verhaltensanalyse. Eine technologisch fortschrittliche Lösung ist besser in der Lage, anspruchsvolle Bedrohungen zu erkennen und darauf zu reagieren.

03

24/7 Überwachung und Reaktion

Cyber-Bedrohungen halten sich nicht an einen Zeitplan. Wählen Sie einen Anbieter, der rund um die Uhr Überwachung und Echtzeit-Reaktion auf Vorfälle bietet, damit Ihr Unternehmen jederzeit geschützt ist.

04

Anpassbarkeit und Skalierbarkeit

Jedes Unternehmen hat einzigartige Sicherheitsanforderungen. Ein zuverlässiger MDR-Anbieter sollte maßgeschneiderte Lösungen anbieten, die mit dem Wachstum Ihres Unternehmens skaliert werden können.

05

Bedrohungsdaten und Forschung

Ein Anbieter, der neuen Bedrohungen immer einen Schritt voraus ist und proaktive Bedrohungsanalysen anbietet, kann Ihrem Unternehmen einen zusätzlichen Schutz bieten.

06

Umgang mit Zwischenfällen und Kommunikation

Ein MDR-Anbieter sollte über klare Protokolle für die Behandlung von Vorfällen und effektive Kommunikationskanäle verfügen, um Sie über den Status von Bedrohungen und Reaktionen zu informieren.

07

Kompetenz bei der Einhaltung von Vorschriften

Wenn Ihre Branche bestimmten Vorschriften unterliegt, stellen Sie sicher, dass der MDR-Anbieter diese kennt und Ihnen helfen kann, die Compliance-Anforderungen zu erfüllen.

08

Fallstudien und Referenzen

Prüfen Sie Fallstudien und suchen Sie nach Referenzen von bestehenden Kunden des Anbieters, um die Auswirkungen und die Effektivität in der Praxis zu beurteilen.

09

Integrationsfähigkeiten

Überlegen Sie, wie gut sich die MDR-Lösung in Ihre vorhandenen Sicherheitstools und -technologien integrieren lässt, um eine umfassende Abdeckung zu gewährleisten.

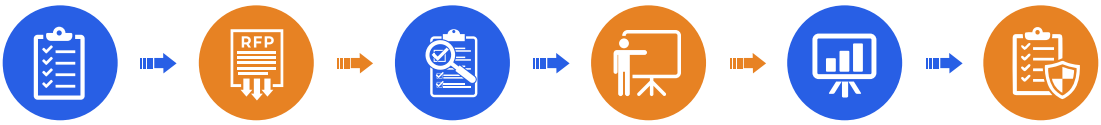
10

Preisgestaltung und Vertragsbedingungen

Informieren Sie sich über die Preisstruktur, ob sie auf einem Abonnement oder auf der Nutzung basiert. Vergewissern Sie sich, dass die Vertragsbedingungen mit Ihrem Budget und Ihren Geschäftsanforderungen übereinstimmen.

Bewerten Sie

Wir haben eine kurze Checkliste für Ihren Bewertungsprozess zusammengestellt:



Recherche und Auswahlliste

Ausschreibung von Angeboten (RFP)

Technische Bewertung

Vorführungen und Präsentationen

Referenzen und Fallstudien

Bewertung der Sicherheit und der Einhaltung von Vorschriften

- **Recherche und Auswahlliste:** Recherchieren Sie potenzielle MDR-Anbieter anhand der Schlüsselfaktoren und erstellen Sie eine Auswahlliste.

- **Ausschreibung von Angeboten (RFP):** Senden Sie RFPs an die in die engere Wahl gekommenen Anbieter, um detaillierte Informationen über ihre Dienstleistungen, Preise und Fähigkeiten zu erhalten.

- **Technische Bewertung:** Führen Sie technische Bewertungen durch, um die Wirksamkeit der Technologie des Anbieters zu beurteilen.

- **Vorführungen und Präsentationen:** Fordern Sie Live-Demonstrationen an, um die MDR-Lösungen in Aktion zu sehen.

- **Referenzen und Fallstudien:** Wenden Sie sich an Referenzen und prüfen Sie Fallstudien, um die Wirkung des Anbieters in der Praxis zu verstehen.

- **Bewertung der Sicherheit und der Einhaltung von Vorschriften:** Bewertung der Sicherheitspraktiken und Compliance-Maßnahmen des Anbieters.

Eine Entscheidung treffen

Bewerten Sie sorgfältig alle gesammelten Informationen, technischen Bewertungen, Referenzen und Vorführungen. Entscheiden Sie sich für einen MDR-Anbieter, der nicht nur Ihre unmittelbaren Anforderungen erfüllt, sondern auch ein Engagement für die langfristige Sicherheit und den Erfolg Ihres Unternehmens zeigt.

Die Auswahl des richtigen MDR-Anbieters ist ein entscheidender Schritt bei der Stärkung der Cybersicherheit in Ihrem Unternehmen. Ein gründlicher Evaluierungsprozess stellt sicher, dass Sie mit einem Anbieter zusammenarbeiten, der nicht nur Ihre einzigartigen Herausforderungen versteht, sondern auch über das Fachwissen und die Technologie verfügt, um Ihr Unternehmen sicher zu machen

Mehr erfahren: https://www.forenova.com/de/managed-detection-and-response-mdr

FORENOVA

Das Unternehmen für 24/7-Bedrohungserkennung

Stärken Sie Ihre Cyber-Resilienz und entlasten Sie Ihr IT-Team mit unseren 24/7-Cybersecurity-Services. Mit einer Kombination aus KI- und Machine-Learning-gesteuerter Technologie und einem erfahrenen Team von Cybersecurity-Spezialisten sind Sie selbst auf die raffinierteste Ransomware-Attacke und jede andere Cyber-Bedrohung vorbereitet.

www.forenova.com