CrowdStrike-Produkte

CROWDSTRIKE

KÄUFERLEITFADEN FÜR VERWALTETE ERKENNUNG UND REAKTION (MDR)

EINFÜHRUNG

WAS IST MDR?

Der chronische Mangel an Cybersicherheitsexperten und Know-how wirkt sich weltweit auf Unternehmen jeder Größe und in allen Branchen aus. Das Problem wird dadurch verschärft, dass Angreifer ihre Praktiken weiterentwickeln, sodass sie immer schnellere und effektivere Angriffe durchführen können. Unternehmen fällt es schwer, den präventiven Sicherheitsansatz hinter sich zu lassen und sich rund um die Uhr auf die Früherkennung von Angriffen, proaktive Bedrohungssuche sowie auf die schnelle und effektive Behebung von Bedrohungen zu konzentrieren. Die Bereitstellung von Personal und Ressourcen für ein eigenes Sicherheitsteam ist für größere Unternehmen mit entsprechenden Budgets sicher kein Problem. Die meisten Unternehmen befinden sich jedoch angesichts ihrer eher begrenzten Mittel in einer schwierigeren Position.

Als Reaktion auf diesen Bedarf wurden Services und Lösungen für verwaltete Bedrohungserkennung und Reaktion (Managed Detection and Response, MDR) entwickelt. MDR unterstützt Unternehmen bei der Implementierung oder Verbesserung von Funktionen zur Bedrohungserkennung, -reaktion und -verwaltung sowie zur kontinuierlichen Überwachung. Die Bereitstellung erfolgt hier als Service.

MDR-Anbieter nutzen endpunktbasierte Detektion und Reaktion (EDR) und andere Technologien, um Transparenz zu sicherheitsbezogenen Ereignissen im gesamten Unternehmen zu schaffen und somit Bedrohungserkennungen sowie Zwischenfalluntersuchungen zu verbessern. Menschliche Analysten überwachen Warnmeldungen und unterstützen Unternehmen bei der Reaktion. Die Reaktion umfasst dabei Aktionen wie die Untersuchung einer Warnmeldung (Triagierung), praktische Maßnahmen zur Reduzierung von Folgen und Risiken (Eindämmung) und schließlich die vollständige Entfernung der Bedrohung sowie die Wiederherstellung eines sicheren Zustands auf dem Endgerät (Behebung).

Eine verantwortungsvolle MDR-Lösung sollte folgende Voraussetzungen erfüllen:

- Ergänzung Ihres Teams mit umfassendem Know-how
- Minutenschnelle Entfernung von Bedrohungen und Übernahme der Behebung
- Deutlich geringe Cybersicherheitsrisiken und Kosten

WARUM BENÖTIGEN UNTERNEHMEN EINEN MDR-SERVICE?

Die Verwaltung eines effektiven Endgeräteschutz-Programms ist teilweise mit erheblichen Herausforderungen verbunden, da die Implementierung sowie die Pflege und Wartung der entsprechenden Tools sehr viel menschliche Arbeit erfordert. Deshalb können viele Unternehmen die Vorteile der von ihnen gekauften Endgeräteschutz-Technologien nicht vollständig ausschöpfen. Für Unternehmen, die eine starke Endgeräteschutz-Verwaltung aufbauen möchten, ist die Situation noch schwieriger, weil mehr Sicherheit aufgrund der höheren Wartungskosten und Verwaltungskomplexität auch mehr Ressourcen erfordert.

Das Ergebnis? Viele Unternehmen verfügen über kein grundlegendes – geschweige denn ein umfassendes – Endgeräteschutz-Programm. Die Situation wird noch verschärft, wenn es zu ernsten Zwischenfällen kommt und das Unternehmen weder die Zeit noch das Know-how besitzt, um das Problem angemessen zu beheben, sodass die Sicherheit des Unternehmens potenziell gefährdet wird.

Folgende Herausforderungen lassen sich mit einem MDR-Service bewältigen:

- **Unternehmen haben Schwierigkeiten bei der vollständigen Implementierung und angemessenen Konfiguration erworbener Technologie.** Je nach Größe und Belastung der IT-Teams fehlen in einigen Unternehmen möglicherweise die nötigen Tools oder die Bandbreite, um die Lösung schnell und ordnungsgemäß auf allen Endgeräten bereitzustellen. Zudem verfügen sie womöglich nicht über die nötige Zeit und das Know-how, um die Richtlinien entsprechend der Sicherheitsanforderungen und der dynamischen Bedrohungslandschaft zu konfigurieren und zu optimieren. Dies kann dazu führen, dass eine Endgerätelösung nur teilweise bereitgestellt und schlecht konfiguriert ist. In der Folge entstehen Sicherheitslücken, die das Unternehmen anfällig für Kompromittierungen machen.

- **Die Anzahl der täglich anfallenden Warnmeldungen und Zwischenfälle ist zu hoch.** Einige Endgeräteschutz-Produkte generieren eine solch enorme Anzahl an Warnmeldungen, dass selbst Unternehmen mit eigenem Sicherheitsteam bzw. Sicherheitskontrollzentrum davon überfordert sein können. Zudem kostet die Verwaltung von Warnungen nicht nur Personal – 67 % der IT-Entscheidungsträger sind der Meinung, dass Sicherheitsprozesse heute mindestens so kompliziert sind wie noch vor zwei Jahren.[1] Leider herrscht in vielen Unternehmen ein Mangel an Fachkräften und Fachwissen, was zu unvalidierten Warnmeldungen und aufsehenerregenden Kompromittierungen führen kann.
- **Unternehmen haben nicht genügend Ressourcen, um Zwischenfälle ordnungsgemäß zu beheben.** Ein Mangel an Ressourcen und Know-how kann dazu führen, dass Unternehmen das Wesen und Ausmaß eines Zwischenfalls nicht rechtzeitig erkennen. 80 % der IT-Entscheidungsträger sind der Meinung, dass der Fachkräftemangel bei Cybersicherheitsexperten ihr Unternehmen anfälliger macht.[2] Unter Umständen werden Zwischenfälle dadurch nicht effizient behoben oder nicht vollständig bzw. schnell genug bearbeitet, was zur Gefährdung oder sogar zur Kompromittierung eines Unternehmens führen kann. Nur mit Können und Erfahrung lässt sich schnell einschätzen, wie ein Zwischenfall am besten behoben werden sollte. Viele Unternehmen, denen es an Ressourcen mangelt, müssen ihre Endgeräte einem mühevollen Re-Imaging-Prozess unterziehen. Die Alternative – punktuelle und kombinierte Gegenmaßnahmen (z. B. Netzwerkeindämmung, Hash-Prävention, Löschen/Bearbeiten von Registrierungswerten oder Stopp/Deaktivierung/Neustart von Diensten) – ist unrealistisch. Zudem lässt sich mit Re-Imaging nicht gewährleisten, dass ein Zwischenfall vollständig behoben wird.
- **Die ordnungsgemäße Implementierung eines Programms erfordert Zeit.** Auch wenn ein Unternehmen über genügend Mittel für die Entwicklung eines internen Endgeräteschutz-Programms verfügt, kann die Umsetzung einer ausgereiften Sicherheitsstrategie einige Zeit in Anspruch nehmen. Es kann Monate, wenn nicht Jahre dauern, die passenden Mitarbeiter zu finden, die geeignete Technologie zu beschaffen, Richtlinien zu definieren und einen Vorfallreaktionsplan aufzustellen. Hinzu kommt, dass solche Programme oft eine niedrigere Priorität als andere, dringliche IT-Projekte haben und Unternehmen durch die sich daraus ergebenden langen Implementierungszeiträume anfällig werden.
- **Es ist schwierig, die nötigen Fachkräfte zu finden und zu halten.** Unternehmen haben mitunter Schwierigkeiten, die nötigen Fachkräfte zu gewinnen, die die Endgeräte effizient schützen können. Laut dem International Information System Security Certification Consortium gibt es weltweit über 3,4 Millionen unbesetzte Stellen für Cybersicherheitsexperten.[3] Selbst Unternehmen mit ausreichenden finanziellen Mitteln haben große Schwierigkeiten mit der Neueinstellung, Schulung und Bindung von Fachkräften, was Reaktionen auf hochentwickelte und raffinierte Bedrohung erschwert. Der Fachkräftemangel ist ein branchenweites Problem.

WAS SIND DIE KERNELEMENTE EINER MDR-LÖSUNG?

MDR-Services dienen hauptsächlich dazu, den Zeitraum zwischen Erkennung und Reaktion zu verringern, sodass die Verweildauer eines Bedrohungsakteurs reduziert und Risiken effektiv minimiert werden. Je schneller der MDR-Anbieter eine Bedrohung erkennt, desto schneller kann die Behebung erfolgen.

Damit eine MDR-Lösung sich dieser Herausforderung erfolgreich stellen und Kunden entsprechende Ergebnisse liefern kann, muss sie über eine Reihe von Kernfunktionen verfügen, die die Bereitstellung schneller Erkennung und Reaktion ermöglichen: eine robuste Plattform, kontinuierliche menschliche Bedrohungssuche, Überwachung und Untersuchung rund um die Uhr sowie punktuelle Behebungsmaßnahmen. Fehlt auch nur eine dieser Kernfunktionen, ist es bedeutend schwieriger, den gesamten Lebenszyklus des Zwischenfalls zu kontrollieren und schnell einen sicheren Zustand wiederherzustellen.

---

1 *Quelle:* ESG 2023 SOC Modernization and the Role XDR report. (https://research.esg-global.com/reportaction/515201525/Toc)
2 *Quelle:* 2023 ESG SOC Modernization and the Role of XDR report. (https://research.esg-global.com/reportaction/515201525/Toc)
3 *Quelle:* 2023 ESG SOC Modernization and the Role of XDR report. (https://research.esg-global.com/reportaction/515201525/Toc)

EINE ROBUSTE PLATTFORM

Robuste Technologien tragen wesentlich zur Bereitstellung einer MDR-Lösung bei, die die gewünschten Ergebnisse liefert. Die Plattform muss Angriffe blockieren und gleichzeitig alle Endgeräteaktivitäten in Echtzeit erfassen und protokollieren, um detaillierte Analysen und Bedrohungssuchen zu ermöglichen.

Eine robuste Plattform besteht aus folgenden Elementen:

1. Eine leicht implementierbare cloudnative Plattform, die Kosten und Komplexität verringert, da sie sofort effektiv eingesetzt werden kann und keine zusätzliche Hardware und Software bzw. Konfiguration erfordert
2. Ein Machine Learning- und Verhaltensanalyse-Modul, das einen vollständigen Echtzeit-Überblick über alle Aktivitäten in der Umgebung bietet
3. Ein einziger schlanker Sensor, der die Plattform mit detaillierten Telemetriedaten aus der gesamten Umgebung versorgt, einschließlich Endgeräte, Cloud-Workloads und Identitäten

Natürlich bietet die Technologie nur dann guten Schutz, wenn sie vollständig bereitgestellt und ordnungsgemäß konfiguriert wurde. Ein MDR-Anbieter sollte seine Erfahrung und bewährten Vorgehensweisen in die Bereitstellung, Konfiguration und Einstellung der Plattform einfließen lassen. Dies wirkt sich deutlich auf den Reifegrad der Sicherheitsmaßnahmen aus und gewährleistet eine sehr schnelle Rendite, da das Onboarding nur wenige Tage und nicht mehrere Wochen dauert.

KONTINUIERLICHE MENSCHLICHE BEDROHUNGSSUCHEN

Durch Bedrohungserkennung können in Ihrer IT-Umgebung viele verschiedene Arten von Schwachstellen aufgedeckt werden. Zumeist erfolgt die Erkennung durch Algorithmen und automatisierte Funktionen, die schnell und effektiv sind und Bedrohungen während der Laufzeit blockieren können. Es gibt jedoch auch Angriffe, die von menschlichen Angreifern gesteuert werden. Sie wissen genau, mit welchen Gegenmaßnahmen ihre Aktivitäten erkannt werden können, und versuchen, diese zu umgehen und somit unerkannt zu bleiben. Die Erkennung dieser verborgenen hochentwickelten Angriffe erfordert ein proaktiveres Vorgehen.

Bei der Bedrohungssuche durchkämmen erfahrene menschliche Analysten kontinuierlich Daten, um kleinste Hinweise auf neue Bedrohungen und hochentwickelte Angriffe aufzuspüren. Diese Hinweise können darauf hindeuten, dass die Angreifer neue Taktiken, Techniken und Prozeduren (TTPs) anwenden und zum Beispiel gestohlene Anmeldedaten zur Nachahmung autorisierter Benutzer verwenden oder versuchen, in der Masse der täglich anfallenden administrativen Aktivitäten unterzutauchen, indem sie systemeigene Tools und Software nutzen.

Ein MDR-Service muss sowohl menschliche Erkennung als auch technologiebasierte Prävention bieten, da sonst nicht alle Möglichkeiten ausgeschöpft werden, um Bedrohungen am Perimeter zu stoppen und unerkannte hochentwickelte Bedrohungen aufzudecken.

ÜBERWACHUNG UND UNTERSUCHUNG RUND UM DIE UHR

Sobald eine Sicherheitswarnung ausgegeben wurde, muss der Sicherheitsanalyst festlegen, welche Maßnahmen – falls nötig – ergriffen werden müssen. Teile des Bedrohungsanalyse-Prozesses lassen sich durch Sandbox-Analysen und Tools zur Verhaltensanalyse automatisieren. Sie liefern verwertbare Informationen und angepasste Kompromittierungsindikatoren (Indicators of Compromise, IOCs) für aufgetretene Bedrohungen.

Viele Aufgaben der Analysephase lassen sich zwar automatisieren, allerdings muss sich der Mensch mit den automatisch generierten Ergebnissen auseinandersetzen und die Richtigkeit, das Ausmaß sowie die Folgen eines Angriffs wirklich verstehen.

Die Erkennung von verborgenen hochentwickelten Angriffen erfordert ein proaktiveres Vorgehen. Bei der Bedrohungssuche durchkämmen menschliche Threat Hunter kontinuierlich die Sicherheitsdaten eines Unternehmens, um kleinste Hinweise auf neue Bedrohungen und hochentwickelte Angriffe aufzuspüren.

Hinzu kommt, dass ein MDR-Service weniger effektiv ist, wenn er den Fokus nur auf die schwerwiegendsten Sicherheitswarnungen legt und Warnungen von mittlerer und geringer Dringlichkeit ignoriert. Fakt ist: Angriffe beginnen häufig mit einer langen Kette von Zwischenfällen mit geringer Dringlichkeit. Werden diese ignoriert, können Angreifer in Ihrem Netzwerk Fuß fassen und sich dort einnisten. Analysiert der MDR-Service alle blockierten Sicherheitserkennungen und -warnungen – also Aktivitäten, die auf einen größeren Angriff hindeuten können –, können Eindringungsversuche so früh wie möglich gestoppt werden.

PRÄZISE BEHEBUNG

Warnungen vor tatsächlichen Bedrohungen für das Unternehmen erfordern eine Reaktion. Die Analyse- und Untersuchungsphasen sollten die nötigen Kontextinformationen für eine angemessene Reaktion liefern.

Die Reaktion kann auf verschiedene Art und Weise erfolgen und zum Beispiel darin bestehen, dass ein Endgerät aus der Umgebung entfernt und eingedämmt wird, um es anschließend in einen sicheren Zustand zurückzuversetzen. In vielen Unternehmen wäre dazu ein Re-Imaging des Endgeräts erforderlich. Mithilfe umfassender Kontextinformationen können kompetente Analysten und effektive Tools das System allerdings auch ohne Re-Imaging in einen sicheren Zustand zurückversetzen. Ein MDR-Anbieter bietet hier einen großen Vorteil, da der Zwischenfall ohne Mitwirkung des Kunden vollständig bewältigt werden kann. Im Vergleich zum Re-Imaging eines ganzen Systems wird der Geschäftsbetrieb weniger beeinträchtigt, zudem ist die Reaktion schneller und mit weniger Kosten verbunden.

Die Behebung bzw. Wiederherstellung stellt die letzte Phase der Zwischenfallreaktion dar. Hierbei werden die Systeme in einen Zustand vor dem Angriff zurückversetzt, d. h. Malware wird entfernt, Registrierungseinträge werden gesäubert und Angreifer bzw. deren Persistenzmechanismen werden beseitigt. Die letzte Phase muss mit besonderer Sorgfalt erfolgen, da ansonsten der Aufwand für die anderen Phasen des MDR-Programms im Prinzip vergebens war. Sobald die Angreifer im Netzwerk Fuß gefasst haben, bedienen sie sich zahlreicher Tricks, um langfristigen Zugang zu erhalten. Mit geplanten Tasks, Überwachungsdiensten sowie redundanten Backdoors und anderen Methoden sorgen sie dafür, dass die Kompromittierung einfachen Quarantäne- und Eindämmungsmaßnahmen widersteht.

Angesichts des breiten Spektrums an sogenannten MDR-Dienstleistungen sollten Sie genau wissen, welche Funktionen ein MDR-Service bieten sollte und inwiefern die angebotenen Funktionen Ihre Anforderungen erfüllen können.

AN WELCHEN KENNZAHLEN SOLLTE SICH IHRE MDR-LÖSUNG ORIENTIEREN?

CrowdStrike hat eine neue Cyberkennzahl definiert, die auf den Erkenntnissen beruht, die wir während der Abwehr von Bedrohungen bei tausenden Unternehmen gewonnen haben: Die „Breakout-Time" gibt die Zeit an, die ein Angreifer benötigt, um sich lateral vom ersten Brückenkopf auf andere Systeme im Netzwerk zu bewegen. Im Jahr 2022 betrug die durchschnittliche Breakout-Time für Cybercrime-Aktivitäten 1 Stunde und 38 Minuten.[5] Doch die Statistik verrät nur einen Teil der Wahrheit: Bei 36 % der erfassten Angriffe beobachtete das OverWatch-Team, dass die Angreifer sich in weniger als 30 Minuten lateral auf weitere Hosts bewegten.

WICHTIG FÜR MDR-KUNDEN: WIR ÜBERNEHMEN VERANTWORTUNG FÜR DAS ERGEBNIS

„Ihr MDR-Anbieter sollte im Rahmen der Reaktionsmaßnahmen für die Behebung verantwortlich sein. Bei der Abwehr von Angriffen spielt Zeit eine entscheidende Rolle. Dazu ist es mitunter erforderlich, das betroffene System vom Netzwerk zu isolieren, Prozesse zu beenden, Persistenzmechanismen aus dem Dateisystem bzw. der Windows-Registrierung zu entfernen, oder eine Vielzahl an Maßnahmen durchzuführen."[2]

4 Crowdstrike-Blog: Does Your MDR Deliver Outcomes – or Homework?

5 CrowdStrike Global Threat Report 2023

Die Breakout-Time verdeutlicht das kurze Zeitfenster, in dem ein Unternehmen am effektivsten verhindern kann, dass sich ein Zwischenfall zu einer Kompromittierung ausweitet. Sicherlich lässt sich nicht nur mit dieser Kennzahl messen, wie raffiniert ein Bedrohungsakteur vorgeht. Dennoch ist ein Vergleich dieses Zeitfensters eine sinnvolle Methode, um die tatsächlichen Fähigkeiten eines Unternehmens zu bewerten. Zudem hilft die Kennzahl Sicherheitsverantwortlichen, die ihre durchschnittliche Erkennungs-, Untersuchungs- sowie Behebungszeit messen und vergleichen wollen. CrowdStrike bezeichnet dies als die „1-10-60-Regel" und empfiehlt Unternehmen, folgende Leistungsvorgaben anzustreben:

- Durchschnittlich 1 Minute bis zur Erkennung eines Angriffs
- Weniger als 10 Minuten, um den Angriff zu untersuchen und zu verstehen
- Weniger als 60 Minuten bis zur Entfernung des Angreifers

Unternehmen, die sich an diesen Vorgaben orientieren, können die Angreifer mit einer höheren Wahrscheinlichkeit aus dem System entfernen, noch bevor diese sich dort festsetzen können, und somit die Folgen des Angriffs abmildern. Natürlich steht es Unternehmen frei, die anzustrebenden Reaktionszeiten an ihre eigenen Bedürfnisse anzupassen. Je nachdem, in welcher Branche und in welchem Land ein Unternehmen tätig ist, könnte die Anpassung auch basierend auf den Angreifern erfolgen, die das Unternehmen am ehesten ins Visier nehmen. Dennoch bietet die 1-10-60-Regel einen Rahmen für die Entwicklung einer MDR-Strategie, mit der jedes Unternehmen seine Fähigkeiten an der betrieblichen Effektivität ausrichten und somit das Vertrauen in die Abwehr von Kompromittierungen stärken kann.

WORAUF SOLLTEN SIE BEI DER WAHL EINER MDR-LÖSUNG ACHTEN?

Hier sind einige Fragen, die bei der Auswahl eines MDR-Services beachtet werden sollten.

Wie hoch ist die Kompetenz der Analysten, die hinter dem MDR-Service stehen?
Ein wichtiges Argument für die Investition in eine MDR-Lösung ist die Verstärkung des eigenen Personals durch Experten, die durch ihre Kompetenz den Reifegrad verbessern, ohne dass dazu teures Personal gesucht und eingestellt werden müsste. CrowdStrike ist optimal aufgestellt, um erfahrene Threat Hunter und Sicherheitsanalysten mit unterschiedlichen Werdegängen (z. B. aus Behörden, Geheimdiensten, Wirtschaftsunternehmen sowie dem Militär) einzustellen sowie zu halten. Das CrowdStrike-Team hat bereits bewiesen, dass es auch äußerst raffinierte Bedrohungen aufspüren und stoppen kann.

Wie lange dauert im Durchschnitt das Onboarding und die Anpassung der MDR-Lösung an die individuellen Bedürfnisse?
Die Umsetzung eines ausgereiften Sicherheitskonzepts ist keine leichte Aufgabe. Nachdem Sie Zeit und Mühe in die Auswahl der richtigen Lösung für Ihr Unternehmen investiert haben, möchten Sie sofort einen Mehrwert sehen und Schutz gewährleisten können. Die Zeitfenster zwischen der Entscheidung für eine Lösung und dem Aufbau der Abwehr ist häufig recht groß und führt dazu, dass das Unternehmen anfällig bleibt bzw. wird. Das Onboarding und die Inbetriebnahme von CrowdStrike Falcon Complete dauert im Durchschnitt nur zehn Tage. Dies verkürzt den Zeitraum bis zum vollständigen Schutz Ihres Unternehmens und zur Umsetzung des versprochenen Mehrwerts.

IST MDR DAS GLEICHE WIE MSSP?

Viele Unternehmen fragen uns: „Benötigen wir einen MDR-Service, wenn wir einen Managed Security Service Provider (MSSP) haben?" MSSP-Angebote können stark variieren. Allgemein liegt deren Schwerpunkt jedoch auf der umfassenden Überwachung und Verwaltung von Sicherheitstools in einem Unternehmen. Dazu gehören in der Regel die einfache Triagierung von Sicherheitswarnungen sowie verschiedene andere Services wie die Verwaltung von Technologie, Upgrades, Compliance und Schwachstellen.

MDR-Services haben dagegen einen sehr viel engeren Aufgabenbereich und lassen sich schnell und ohne weiteren Aufwand mit speziellen Technologien integrieren. Zudem sind MDR-Services auf eine bestimmte Aufgabe ausgelegt und sollen das Sicherheitskontrollzentrum eines Unternehmen bei konkreten Schritten der Erkennungs- bzw. Reaktions-Workflows unterstützen. Aufgrund dieses engen Fokus bietet eine MDR-Lösung in sehr kurzer Zeit unmittelbaren Mehrwert zu geringen Kosten.

Welche automatisierten präventiven Technologien enthält die MDR-Lösung?
Eine umfassende MDR-Lösung, die mit Ihrem Unternehmen heute und in der Zukunft skalieren kann, sollte die Vorteile automatisierter und präventiver Technologien nutzen. Die CrowdStrike Falcon®-Plattform nutzt die CrowdStrike Security Cloud und erstklassige künstliche Intelligenz, um Echtzeit-Angriffsindikatoren, Bedrohungsanalysen, veränderte Vorgehensweisen von Angreifern sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen auszuwerten. Dadurch kann die CrowdStrike-Plattform äußerst präzise Bedrohungen erkennen, automatisierte Schutz- und Behebungsmaßnahmen bereitstellen, zuverlässige Bedrohungssuchen durchführen und Schwachstellen priorisieren. Dies ermöglicht schnelle und skalierbare Bereitstellung, hervorragende Schutzwirkung und Geschwindigkeit, geringere Komplexität sowie sofortige Rendite.

Bietet Ihre MDR-Lösung verwalteten und cloudbasierten Schutz vor Identitätsbedrohungen?
Bei 80 % aller Angriffe werden heute kompromittierte Anmeldedaten genutzt. Solche identitätsbasierten Angriffe lassen sich jedoch mit herkömmlichen Sicherheitsansätzen kaum aufdecken. Wenn die Anmeldedaten eines zulässigen Benutzers kompromittiert wurden und sich ein Bedrohungsakteur als dieser Benutzer tarnt, ist es oft sehr schwer, zwischen dem typischen Verhalten des Benutzers und dem des Hackers zu unterscheiden. Mit Falcon Complete Identity Threat Protection (ITP) ist das aber kein Problem. ITP ist der erste und bislang einzige vollständig verwaltete Identitätsschutz-Service, der rund um die Uhr reibungslosen Echtzeitschutz vor Identitätsbedrohungen bietet – mit erweiterter IT-Richtliniendurchsetzung für verwaltete und nicht verwaltete Konten sowie Verwaltung, Überwachung und Behebung durch Experten.

Profitiert Ihr MDR-Service von integrierten und nativen Bedrohungsanalysen?
Um neue Bedrohungen mit größtmöglicher Wirksamkeit erkennen und darauf reagieren zu können, müssen Sicherheitsanalysten aktuelle Informationen über die neuesten TTPs besitzen, die von den aktiven Bedrohungsakteuren verwendet werden. Die CrowdStrike-MDR-Services nutzen Cyber-Bedrohungsanalysen, die das CrowdStrike-Expertenteam erstellt hat. Das CrowdStrike Intelligence-Team besteht aus Sicherheitsforschern, Kulturexperten sowie Linguisten und unterstützt den MDR-Prozess mit detaillierten, stets aktuellen Informationen über die Vorgehensweisen von über 200 Angreifern. Dank diesem detaillierten Wissen zu den neuesten TTPs kann CrowdStrike Bedrohungen effektiv und effizient erkennen und darauf reagieren.

Wie kommunizieren Ihre MDR-Experten mit unserem Team?
Bei allen MDR-Services gibt es eine Phase im Erkennungs-/Untersuchungs-/Reaktions-Workflow, in der die Kontrolle an Sie zurückgegeben wird. Die Kommunikation dieser Übergabe stellt einen potenziellen Reibungspunkt dar, da einige Anbieter hier neue Konsolen, Portale oder Workflows einführen, die die Reaktion Ihres Teams verlangsamen. Ein zentrales Hub, das die nahtlose Bereitstellung von Informationen zwischen MDR-Anbieter und Kunden ermöglicht, ist daher unverzichtbar. Das CrowdStrike Message Center reduziert Reibungsverluste in der MDR-bezogenen Zusammenarbeit und ermöglicht eine reibungslose, transparente sowie sichere Kommunikation zwischen den Analysten der CrowdStrike Managed Services und den Kunden. Über das in die Falcon-Plattform integrierte Message Center können die CrowdStrike-Analysten die Kunden in Echtzeit über gerade stattfindende Angriffe und damit verbundene Aktivitäten benachrichtigen, sodass die Kunden jederzeit umfassend über Angriffsaktivitäten und die erforderlichen Gegenmaßnahmen informiert sind. Die Kommunikation erfolgt in beide Richtungen und vereinfacht den Informationsaustausch sowie die Zusammenarbeit zwischen CrowdStrike und den Analysten beim Kunden innerhalb der Falcon-Plattform.

Welche Reaktionsmaßnahmen übernimmt die MDR-Lösung und für welche Maßnahmen sind die Kunden verantwortlich?
Der Begriff Reaktion kann häufig viele Dinge bedeuten und sorgt auf dem Markt für Verwirrung, da nicht genau definiert ist, welche Leistungen MDR-Anbieter übernehmen und welche zusätzliche Arbeit die Kunden im Anschluss noch erledigen müssen. Eine MDR-Lösung muss in der Lage sein, einen Angreifer zu isolieren, einzudämmen und vollständig aus der Umgebung zu entfernen. Bei der Entfernung wechselt häufig die Verantwortung – was für die Kunden zu deutlich mehr Arbeitsaufwand über die Isolierung und Eindämmung hinaus führen kann. Falcon Complete übernimmt die letzte Phase für Sie und geht bei der Reaktion noch einen Schritt weiter: CrowdStrike führt Isolierung, Eindämmung und – sofern möglich – auch die Behebung durch.

Services zur Bedrohungsbeseitigung sollten Systeme nahtlos auf einen Zustand vor dem Angriff zurücksetzen und dabei Malware entfernen, die Registrierungen säubern und Angreifer sowie Persistenzmechanismen entfernen – und dabei nach Möglichkeit zeitintensives Re-Imaging vermeiden.

Das beinhaltet das Entfernen schädlicher Dateien, Artefakte und Prozesse aus der Umgebung sowie die sofortige Wiederherstellung eines sicheren Zustands im gesamten Unternehmen. Dadurch erhalten die Kunden Ergebnisse und keine zusätzliche Arbeit.

Ist der MDR-Service rund um die Uhr verfügbar?
Angreifer machen keinen Urlaub, weshalb auch Ihr MDR-Service stets verfügbar sein sollte. Mitunter entscheiden sich viele Unternehmen aufgrund des Rund-um-die-Uhr-Bedrohungsschutzes für einen MDR-Service, vor allem wenn das eigene Team nur zu den Geschäftszeiten arbeitet.

Kann der MDR-Anbieter nicht nur Risiken, sondern auch Kosten reduzieren?
Wenn Sie die individuellen Ergebnisse Ihrer MDR-Lösung verstehen, können Sie besser einschätzen, ob die Lösung Risiken minimieren kann und wie Zwischenfälle den Gewinn Ihres Unternehmens beeinträchtigen könnten. CrowdStrike hat nur eine Mission: Wir stoppen Angriffe. Falcon Complete verwaltet den gesamten Lebenszyklus eines Zwischenfalls und gewährleistet eine Beweiskette für alle Sicherheitszwischenfälle, damit sich die CrowdStrike-Experten rund um die Uhr einzig und allein auf das Stoppen von Kompromittierungen konzentrieren können. Zudem zeigte eine im Jahr 2021 **von CrowdStrike bei Forrester in Auftrag gegebene Untersuchung der wirtschaftlichen Auswirkungen**, dass Falcon Complete mehr als 400 % Rendite bietet und Ihrem Unternehmen jährlich über 2.500 Arbeitsstunden für Untersuchungen spart.

In welcher Form wird garantiert, dass die MDR-Lösung wirklich zuverlässig schützt?
Es ist durchaus üblich, dass ein MDR-Service behauptet, Sie vor Cyberangriffen schützen zu können. Dann stellt sich die Frage: „Woher weiß ich, dass das auch umgesetzt wird?“ Ein Anbieter, der nicht überzeugend darlegen kann, wie er diese Behauptungen und deren Umsetzung beweisen kann, muss Misstrauen erwecken. CrowdStrike hat daher als erster Anbieter eine **Garantie für die Verhinderung von Kompromittierungen** eingeführt. CrowdStrike ist absolut davon überzeugt, dass unsere Lösungen Kompromittierungen zuverlässig stoppen, und übernimmt die Kosten, falls es tatsächlich zu einer Kompromittierung kommt. Dies zeigt unser Vertrauen in die Zuverlässigkeit des Falcon Complete MDR-Services.

Wurde der MDR-Service durch Dritte validiert?
Häufig ist die Evaluierung von MDR-Lösungen ein mühsamer Prozess, der kein klares Ergebnis dazu liefert, welche Lösung für Ihr Unternehmen die richtige ist. Viele Anbieter versprechen die gleichen Leistungen und Ergebnisse. Im Rahmen Ihrer Evaluierung sollten Sie sich daher fragen: „Gibt es für diesen MDR-Service Validierungen durch Dritte und wie helfen mir diese Analysen bei meiner Entscheidung?“ CrowdStrike ist stolz darauf, sowohl im Forrester Wave-Report als auch von IDC MarketScape als führender Anbieter (Leader) für MDR ausgezeichnet worden zu sein. Außerdem haben wir bei den MITRE Engenuity ATT&CK®-Bewertungen 2022 für Security-Service-Anbieter die beste Erkennungsabdeckung erreicht. Bei der Bewertung von MDR-Lösungen sollten Sie sich an diesen Experten orientieren.

Wie häufig beteiligt sich der MDR-Anbieter an der Verwaltung und Optimierung des MDR-Services?
Für die Abwehr moderner Bedrohungen sind kontinuierliche Verbesserung und Optimierung unerlässlich. Da Angreifer täglich schneller und raffinierter werden, muss Ihr MDR-Service bei der Verwaltung und Optimierung Ihrer MDR-bezogenen Plattform, Richtlinien sowie Prozesse eine bedeutende und umfassende Rolle spielen. Dies gewährleistet die konsequente Optimierung des Services und beim Stoppen von Kompromittierungen zuverlässige Ergebnisse.

FALCON COMPLETE: EINE UMFASSENDE UND HOCHEFFEKTIVE MDR-LÖSUNG

CrowdStrike Falcon® Complete für Verwaltete Erkennung und Reaktion (Managed Detection and Response, MDR) verbindet die Vorteile der branchenführenden und cloudnativen Falcon-Sicherheitsplattform mit der Effizienz, Expertise und dem Rund-um-die-Uhr-Schutz der weltweiten CrowdStrike-Sicherheitsexperten, die jede Bedrohung für Kundenunternehmen kontinuierlich überwachen, einschätzen und abwehren.

Funktionen	Falcon Complete MDR
Verwaltung und Optimierung rund um die Uhr	
Betrieb durch Experten	✓
Proaktive Plattformverwaltung	✓
Zugewiesener Sicherheitsberater	✓
Priorisierung der Ressourcengruppen	✓
Interdisziplinäres Know-how	✓
Erkennung und Prävention	
Kontinuierliche Überwachung mit Echtzeit-Überblick	✓
Untersuchung aller Erkennungen (niedrig, mittel, hoch, kritisch)	✓
Spezialisierte Daten, Tools und Prozesse	✓
Verwalteter Cloud-Workload-Schutz	✓
Verwalteter Schutz vor Identitätsbedrohungen	✓
Bedrohungssuche und Bedrohungsanalyse	
Native Bedrohungsanalysen und integrierte IOCs	✓
Vierteljährliche Berichte über Bedrohungssuchen	
Vollständiger Überblick über den Prozessbaum für alle Endgeräte	✓
Proaktive menschliche Bedrohungssuche rund um die Uhr	✓
Proaktive menschliche Bedrohungssuche rund um die Uhr	
Isolierung und Eindämmung aller Bedrohungen	✓
Proaktive manuelle und punktuelle Behebung	✓

IHRE MDR-LÖSUNG SOLLTE ERGEBNISSE LIEFERN – UND NICHT ZUSÄTZLICHE ARBEIT

Die Ergebnisse sollte der MDR-Anbieter erbringen, nicht der Kunde. Falcon Complete übernimmt die volle Verantwortung für die Ergebnisse.

In der Regel wollen Kunden einen MDR-Service vor allem aus einem einfachen Grund: Sie möchten eine schädliche Kompromittierung vermeiden. Da viele MDR-Anbieter dieses Ergebnis nicht versprechen können, teilen sie die Anforderungen häufig in einzelne Verpflichtungen auf (z. B. wie schnell ein Analyst auf eine kritische Warnung reagiert). Service Level Agreements (SLAs) wie diese eignen sich, um die Effektivität über einen längeren Zeitraum einzuschätzen, wobei SLA-Versprechen mit kurzen Reaktionszeiten tatsächlich das Risiko einer Kompromittierung minimieren können. Damit verpflichten sich die Anbieter aber noch lange nicht dazu, ihren Hauptauftrag – das Stoppen von Angriffen – zu erfüllen.

Vom ersten Tag an umfasst Falcon Complete eine erstklassige Garantie für die Verhinderung von Kompromittierungen. Dadurch können Kunden darauf vertrauen, dass CrowdStrike von seinem Team und den gelieferten Ergebnissen absolut überzeugt ist.

Heute gibt es eine Vielzahl an MDR-Services. Wenn Sie eine Lösung zur Ergänzung Ihres eigenes Sicherheitsteams suchen, sollten Sie zunächst wissen, wie gut Ihr Team Bedrohungen erkennen, untersuchen und darauf reagieren kann – und wo die Schwächen Ihres Teams liegen. Anschließend sollten Sie bewerten, wie gut die MDR-Lösung die Bereiche Mitarbeiter, Prozesse und Technologien abdecken kann. So können Sie einschätzen, ob Ihr MDR-Anbieter Ihnen eine Aufforderung zu nächsten Schritten schickt (zusätzliche Arbeit) oder sie lediglich darüber informiert, dass die Bedrohung entfernt und behoben wurde (Ergebnis). Daran können Sie erkennen, ob der Anbieter Kompromittierungen, die Ihr Unternehmen gefährden, stoppen kann.

Demo zu Falcon Complete MDR vereinbaren

Weitere Informationen unter **www.crowdstrike.de**

ÜBER CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit einer der weltweit fortschrittlichsten cloudnativen Plattformen für Endgeräte- und Workloadschutz sowie Identität und Daten die Sicherheit geschäftskritischer Unternehmensbereiche neu.

Die CrowdStrike Falcon®-Plattform nutzt die CrowdStrike Security Cloud und erstklassige KI, um Echtzeit-Angriffsindikatoren, Bedrohungsanalysen, veränderte Vorgehensweisen von Angreifern sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen auszuwerten. Dadurch kann die CrowdStrike-Plattform äußerst präzise Bedrohungen erkennen, automatisierte Schutz- und Behebungsmaßnahmen bereitstellen, zuverlässige Bedrohungssuchen durchführen und Schwachstellen priorisieren.

CrowdStrike Falcon® wurde für den Cloud-Einsatz entwickelt und nutzt einen einzigen schlanken Agenten, um schnelle und skalierbare Bereitstellung, hervorragende Schutzwirkung und Geschwindigkeit, geringere Komplexität sowie sofortige Rendite zu ermöglichen.

Das Motto von CrowdStrike lautet: **We stop breaches.**

Folgen Sie uns: **Blog | Twitter | LinkedIn | Facebook | Instagram**