CROWDSTRIKE

MANAGED DETECTION AND RESPONSE (MDR) EIN LEITFADEN FÜR DIE BESCHAFFUNG

EINLEITUNG

WAS VERSTEHT MAN UNTER MDR?

In allen Branchen herrscht bekanntermaßen ein chronischer Mangel an Fachkräften und Know-how im Bereich der Internetsicherheit. Das Problem gilt weltweit und betrifft Organisationen jeder Größenordnung. Dass Angreifer ständig ihre Techniken verbessern und Angriffe mit hoher Geschwindigkeit und großer Wirkung ausführen, macht es nur schlimmer. Auf der anderen Seite fällt es Unternehmen und Institutionen schwer, mehr zu tun als präventive Sicherheitsmaßnahmen zu ergreifen. Es fehlt an der Fähigkeit zur früheren Erkennung, zur proaktiven Bedrohungssuche und zur schnellen und wirksamen Reaktion auf Bedrohungen rund um die Uhr. Die personelle und finanzielle Ausstattung eines engagierten Sicherheitsteams, das diese Anforderungen erfüllt, mag für größere Organisationen mit den entsprechenden Budgets machbar sein. Für die meisten Unternehmen ist dies allerdings aufgrund ihrer begrenzten Ressourcen keine realistische Option.

Managed Detection and Response (MDR) ist ein Service, der aus dem Bedarf der Märkte entstanden ist. MDR implementiert oder verbessert die Fähigkeit von Organisationen zur Erkennung, Reaktion, Verwaltung und kontinuierlichen Überwachung von Bedrohungen.

Im *Market Guide for Managed Detection and Response Services* vom 15. Juli 2019 nennt Gartner Research das Ziel von MDR: „MDR-Services zielen darauf ab, Auswirkungen von Sicherheitsvorfällen auf die Kunden schnell zu erkennen und zu begrenzen. Diese Services konzentrieren sich rund um die Uhr auf die Fernüberwachung und -erkennung von Bedrohungen ebenso wie auf gezielte Gegenmaßnahmen. MDR-Anbieter nutzen für die Nachforschung, die Bedrohungssuche und die Reaktion auf erkannte Bedrohungen ggf. eine Kombination aus Technologien auf Host- und Netzwerkebene, ebenso wie hochentwickelte Analysen, Bedrohungsaufklärung, forensische Daten und menschliches Fachwissen.“*

Ein MDR-Anbieter setzt üblicherweise ein Tool für die Endgeräteerkennung und Reaktion (EDR) ein, um einen Einblick in sicherheitsrelevante Ereignisse am Endgerät zu erhalten und so die Erkennung von Bedrohungen und die Untersuchung von Vorfällen zu flankieren. Parallel dazu überwachen Experten die Warnmeldungen und unterstützen bei Abhilfemaßnahmen. Dies kann die Untersuchung von Alarmen (Triage) umfassen, die Risikominderung und die vollständige Beseitigung der Bedrohung mit gleichzeitiger Wiederherstellung des Endgeräts in einen einwandfreien Zustand (Abhilfe).

WAS MACHT MDR-SERVICES SO WICHTIG?

Ein wirksames Programm zur Endgerätesicherheit praktisch umzusetzen, kann schwierig sein. Die notwendigen Werkzeuge setzen oft detaillierte Kenntnisse voraus. Zudem verlangen richtige Implementierung, Unterstützung und Wartung oft umfangreiche personelle Ressourcen. Daher gelingt es vielen Unternehmen und Institutionen nicht, die erworbenen Technologien für die Endgerätesicherheit vollständig zu nutzen. Noch schwieriger sieht es für Organisationen aus, die die geltenden Empfehlungen für die Endgeräte-Sicherheitslage umsetzen möchten. Denn ein höheres Sicherheitsniveau erfordert noch mehr Ressourcen, da Wartung und Administration ggf. noch komplexer sind.

Das Ergebnis? Vielen Unternehmen und Institutionen gelingt es nicht, ein grundlegendes Endgerätesicherheitsprogramm erfolgreich zu implementieren – ganz zu schweigen von einem wirklich umfassenden Schutz. Kritisch wird es, wenn schwere Sicherheitsvorfälle auftreten und die Organisation nicht die Zeit oder das Fachwissen zur Behebung der Probleme hat, was für die Organisation existenzgefährdend werden kann.

“MDR-Services zielen darauf ab, Auswirkungen von Sicherheitsvorfällen auf die Kunden schnell zu erkennen und zu begrenzen. Diese Services konzentrieren sich rund um die Uhr auf die Fernüberwachung und -erkennung von Bedrohungen ebenso wie auf gezielte Gegenmaßnahmen. MDR-Anbieter nutzen für die Nachforschung, die Bedrohungssuche und die Reaktion auf erkannte Bedrohungen ggf. eine Kombination aus Technologien auf Host- und Netzwerkebene, ebenso wie hochentwickelte Analysen, Bedrohungsaufklärung, forensische Daten und menschliches Fachwissen.”

Gartner Research, Market Guide for Managed Detection and Response Services, 15. Juli 2019

* Gartner Research, Market Guide for Managed Detection and Response Services, 15. Juli 2019, von Craig Lawson, Toby Bussa, Sid Deshpande, Pete Shoard, Kelly Kavanagh

MDR BESCHAFFUNGSLEITFADEN

Bei der Implementierung eines Endgerätesicherheitsprogramms treten oft insbesondere folgende Probleme auf:

- **Organisationen haben Schwierigkeiten bei der vollständigen Implementierung und korrekten Konfiguration der erworbenen Technologie.**
  Je nach Größe und Arbeitsbelastung der IT-Teams fehlt es Unternehmen nicht selten an Werkzeugen und Bandbreite zur schnellen und erfolgreichen Implementierung der Lösung auf den Endgeräten. Darüber hinaus fehlen Zeit und Fachwissen zur ordnungsgemäßen Konfiguration und Abstimmung von Richtlinien, die den Sicherheitsanforderungen entsprechen und den Schutz der Endgeräte auch bei Veränderungen der Bedrohungslage gewährleisten. Diese Situation kann dazu führen, dass die Endgerätelösung nur unvollständig bereitgestellt und lückenhaft konfiguriert wird. Das macht die Organisation anfällig für Sicherheitsverletzungen.

- **Die Zahl der täglichen Alarme und Vorfälle ist zu hoch.** Der Umgang mit der oft großen Zahl von Alarmen, die von einigen Endgerätesicherheitslösungen erzeugt werden, kann selbst Unternehmen überfordern, die über ein eigenes Sicherheitsteam oder Security Operation Center verfügen. Die richtige Interpretation der Alarme erfordert nicht nur ausreichendes Personal, sondern auch Mitarbeiter mit entsprechenden Kenntnissen im Bereich der Internetsicherheit, die die Meldungen verstehen und die richtigen Entscheidungen treffen. Dem steht meist die knappe Personaldecke entgegen, sodass Alarme unbeachtet bleiben, was versierten Angreifern Tür und Tor öffnet.

- **Organisationen haben nicht die Ressourcen, um Vorfälle einwandfrei zu beheben.** Knappe Ressourcen und fehlendes Spezialwissen können dazu führen, dass sich Organisationen schwer damit tun, Art und Umfang eines Vorfalls rechtzeitig richtig einzuordnen. Vorfälle können dann nicht effizient behoben, nicht vollständig angegangen oder nicht rechtzeitig behandelt werden – mit entsprechenden Folgen für die Sicherheitslage. Die richtige Behebung von Vorfällen verlangt Fertigkeiten und Erfahrung. Vielen Unternehmen und Institutionen fehlt es an den nötigen Ressourcen. Sie sind daher gezwungen, ihre Endgeräte neu aufzusetzen. Alternativen, wie beispielsweise Netzwerkeindämmung, Hash-Prävention, Löschen/Ändern von Registrierungsschlüsselwerten oder Stoppen/Deaktivieren/Neustarten von Diensten, kommen für sie aus den genannten Gründen nicht infrage. Doch selbst ein Re-Imaging ist keine Gewähr dafür, dass der Vorfall anschließend vollständig behoben ist.

- **Die erfolgreiche Implementierung eines Programms braucht Zeit.** Selbst wenn die finanziellen Mittel für den Aufbau eines internen Endgerätesicherheitsprogramms vorhanden sind, kann sich die Umsetzung einer ausgereiften Sicherheitsstrategie hinziehen. Von der Suche und Einstellung des geeigneten Personals und dem Erwerb der entsprechenden Technologie bis hin zur Festlegung von Richtlinien und der Definition von Prozessen zur Reaktion auf Vorfälle (IR) können Monate, wenn nicht Jahre vergehen. Zudem wird derartigen Programmen oft eine geringere Priorität eingeräumt als anderen dringenden IT-Projekten. Das führt zu langen Implementierungsprozessen und macht die Unternehmen verwundbar.

- **Es ist schwer, Personal mit dem notwendigen Fachwissen zu finden und zu halten.** Es ist nicht einfach, das erforderliche Fachpersonal für eine effiziente Sicherung der Endgeräte an Bord zu holen. **Der Marktforschungsbericht** der Enterprise Strategy Group zeigt, dass 74 % der Unternehmen und Institutionen vom Mangel an Fachkenntnissen im Bereich der Internetsicherheit stark oder relativ stark betroffen sind. Eine weitere Problematik ist die Bindung der Mitarbeiter und die notwendige fortlaufende Schulung entsprechend der immer anspruchsvolleren Bedrohungslandschaft. Der Fachkräftemangel ist ein branchenweites Problem.

"Bis 2024 werden 25 % der Organisationen die MDR-Dienste in Anspruch nehmen, gegenüber weniger als 5 % derzeit.

Bis 2024 werden 40 % der mittelständischen Unternehmen MDR-Dienste als ihren einzigen verwalteten Sicherheitsdienst nutzen."

Gartner Research, Market Guide for Managed Detection and Response Services, 15. Juli 2019

DIE KERNELEMENTE VON MDR

Die MDR-Angebote zeichnen sich durch eine Vielzahl unterschiedlicher Leistungsmerkmale aus, die sich zudem im Laufe der Zeit weiterentwickeln. Es gibt jedoch gewisse Kernbestandteile:

ERKENNUNG

Die Bedrohungserkennung bildet die Grundlage jedes MDR-Service. Der Fokus liegt hier darauf, Angriffe zu erkennen, die die vorhandenen Sicherheitskontrollen umlaufen haben. Dass die präventiven Kontrollen nicht greifen, kann verschiedene Ursachen haben: Angreifer wenden neue oder neuartige Taktiken, Techniken und Verfahren (TTPs) an, die Abwehrsysteme wurden nicht einwandfrei konfiguriert oder es wurden erst gar keine präventiven Maßnahmen zum Schutz der Endgeräte implementiert.

Meistens stützt sich die Erkennung auf schnelle und wirksame Algorithmen und automatisierte Prozesse. Manche Angriffe werden aber auch von Angreifern ausgeführt, die die Gegenmaßnahmen gut kennen und diesen aktiv ausweichen, um verborgen zu bleiben. Das Erkennen versteckter versierter Angriffe verlangt eine proaktivere Vorgehensweise. Bei der Bedrohungssuche durchforsten Experten kontinuierlich die Sicherheitsdaten von Unternehmen auf der Suche nach ersten Anzeichen für aufkommende Bedrohungen und Angriffe.

PRIORISIERUNG

Viele Organisationen sind mit einer schier unüberschaubaren Anzahl von Warnmeldungen konfrontiert, die sich auf eine stetig wachsende Zahl von Endgeräten beziehen. Sicherheitsverantwortliche, die diese Arbeitslast effizient und effektiv bewältigen wollen, müssen Prioritäten setzen. Dazu benötigen sie zusätzlichen Kontext, der sich aus Bedrohungsanalysen und erweiterten Datenanalysen ableitet. So lässt sich einschätzen, wann ein Sicherheitsvorfall gravierende Auswirkungen haben könnte. Zumindest aber müssen die Sicherheitsverantwortlichen wissen, welche Daten und Assets besonders sensibel und schutzbedürftig sind.

UNTERSUCHUNG

Sobald die Prioritäten festgelegt sind, wird der Alarm analysiert, um festzustellen, ob es sich um eine Falschmeldung handelt. Von diesem wichtigen Schritt hängt ab, welche Sicherheitsmaßnahmen ergriffen werden müssen. Bestimmte Teilbereiche der Bedrohungsanalyse lassen sich mit Sandboxing automatisieren – oder auch mit Verhaltensanalysetechniken. Diese liefern fundierte Informationen und individuelle Gefährdungsindikatoren (Indicators of Compromise) für die aufgetretenen Bedrohungen.

Viele Aufgaben in der Analysephase können automatisiert werden. Doch um das Risiko, das Ausmaß und die Auswirkungen eines Angriffs wirklich verstehen zu können, ist die Einschätzung von Experten erforderlich – auch was die automatisch erzeugten Auswertungen angeht.

REAKTION

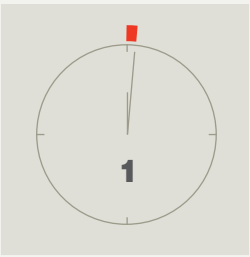
Wenn sich eine Warnung als Bedrohung erweist, muss die Organisation reagieren. Aus der Analyse- und Untersuchungsphase stammt der notwendige Kontext zur Einschätzung, welche Reaktion erforderlich ist. Die Reaktion kann viele Formen annehmen, z. B. die Notwendigkeit, ein Endgerät aus der Umgebung zu entfernen und zu isolieren, sodass man zu einem bekannt guten Zustand zurückkehren kann. Viele Organisationen greifen hierzu auf ein Re-Imaging des Endgeräts zurück. Wenn allerdings fundierte Kontextinformationen vorliegen, können qualifizierte Analysten mit wirksamen Tools das System auch ohne ein Re-Imaging wieder in einen einwandfreien Zustand versetzen. Diese Vorgehensweise vermeidet Beeinträchtigungen der Geschäftsprozesse und ist zudem schneller als ein vollständiges Re-Imaging des gesamten Systems.

Das Erkennen versteckter versierter Angriffe verlangt eine proaktivere Vorgehensweise. Bei der Bedrohungssuche durchforsten Experten kontinuierlich die Sicherheitsdaten von Unternehmen auf der Suche nach ersten Anzeichen für aufkommende Bedrohungen und Angriffe.

WELCHE METRIKEN SOLLTEN EINEM MDR-SERVICE ZUGRUNDELIEGEN?

CrowdStrike® ist Vorreiter bei der Einführung einer neuen Cyber-Metrik. Diese stützt sich auf Erkenntnisse aus der Hilfe für Tausende Organisationen bei der Abwehr von Bedrohungen und wird als „Breakout Time" bezeichnet. „Breakout Time" ist die durchschnittliche Zeit, die ein Angreifer braucht, um sich von einer kompromittierten Maschine lateral weiter durch das Netzwerk seines Opfers zu bewegen. Die gesamte durchschnittliche Breakout Time, die CrowdStrike 2018 über alle Einbrüche und Bedrohungsakteure hinweg beobachtete, betrug 4 Stunden und 37 Minuten. Diese Statistik erzählt allerdings nicht die ganze Geschichte: Denn CrowdStrike beobachtete bemerkenswerte Unterschiede zwischen einzelnen Angreifergruppen, und zwar von durchschnittlich 9 Stunden und 42 Minuten für eCrime-Angreifer bis hin zu erstaunlichen 18 Minuten für russische Bedrohungsakteure.

Die Breakout Time wirft ein Schlaglicht auf das enge Zeitfenster, in dem eine Organisation verhindern kann, dass ein Vorfall zu einer Sicherheitsverletzung wird. Die Breakout Time ist sicherlich nicht die einzige Metrik, nach der man die Geschicklichkeit von Bedrohungsakteuren beurteilen kann, aber sie ist eine gute Möglichkeit, deren operative Fähigkeiten zu bewerten. Sie ist auch insofern für Verteidiger nützlich, die die mittlere Zeit bis zur Erkennung, Untersuchung und Behebung messen möchten. CrowdStrike nennt dies die „1-10-60-Regel" und empfiehlt Unternehmen und Institutionen die Einhaltung folgender Leistungskennzahlen:



In durchschnittlich 1 Minute ein Eindringen erkennen

In weniger als 10 Minuten im Bilde sein

In weniger als 60 Minuten den Angreifer herauswerfen

Anforderungen anpassen. Das hängt auch davon ab, mit welchem Typ von Angreifer sie aufgrund ihrer Branche und Region am ehesten rechnen müssen. Bei der Umsetzung einer MDR-Strategie bietet die 1-10-60-Regel jedoch einen Rahmen, der es jeder Organisation ermöglicht, sich so aufzustellen, dass sie Sicherheitsverletzungen entsprechend ihren Fähigkeiten wirksam stoppen kann.

IST MDR DASSELBE WIE MSSP?

Viele Organisationen stellen sich die Frage: „Brauche ich überhaupt einen MDR-Service, wenn ich doch mit einem Managed Security Service Provider (MSS-Provider) arbeite?" Das Leistungsangebot von MSS-Providern kann sehr unterschiedlich sein. Im Allgemeinen widmen sich diese Provider der umfassenden Überwachung und Verwaltung von Sicherheitswerkzeugen in einem Unternehmen. Dazu gehört üblicherweise die grundlegende Priorisierung von Sicherheitswarnungen zusammen mit einer Vielzahl anderer Services, wie Technologie-Management und -Upgrades, Compliance und Schwachstellen-management.

Im Unterschied dazu ist ein MDR-Service deutlich enger gefasst. MDR stellt eine schnelle schlüsselfertige Integration bereit – in der Regel für einen bestimmten Technologiestack. MDR-Services konzentrieren sich zudem stärker auf ihren Auftrag. Sie zielen in der Regel darauf ab, das Security Operation Center einer Organisation in bestimmten Arbeitsabläufen bei der Erkennung und Abwehr von Bedrohungen zu unterstützen. Aufgrund dieser Fokussierung kann MDR einen sofortigen Nutzen zu geringen Kosten innerhalb eines sehr kurzen Zeitfensters bieten. Im kürzlich erschienenen Market Guide for Managed Detection and Response Services vom 15. Juli 2019 schätzt Gartner Research, dass bis 2024 rund 40 % der mittelständischen Unternehmen MDR-Dienste als ihren einzigen verwalteten Sicherheitsdienst nutzen werden.

WELCHE HAUPTKATEGORIEN DECKEN DIE AKTUELLEN MDR-SERVICES AB?

Es gibt viele verschiedene Arten von Diensten, die unter die Bezeichnung MDR fallen, beispielsweise:

VERWALTETE PRIORISIERUNG

Verwaltete Priorisierung (Managed Prioritization) konzentriert sich auf die Verwaltung und Triage von Sicherheitswarnungen. Da dies meist die Warnmeldungen von EDR-Lösungen betrifft, werden diese Dienste auch oft als Managed EDR bezeichnet. Die Priorisierung ergänzt die Maßnahmen, die typischerweise von Experten auf Ebene 1 in Organisationen mit einem dedizierten SOC ergriffen werden. Ein Service mit verwalteter Priorisierung senkt die Anzahl der Alarme, die vom Sicherheitspersonal überprüft werden müssen. Hierzu dienen automatisierte Regeln in Verbindung mit Fachleuten, die potenzielle Vorfälle prüfen und harmlose sowie falsch-positive Meldungen aussortieren. Der Service kann Warnmeldungen mit zusätzlichem Kontext versehen, sodass sich ein potenzieller Vorfall besser einordnen lässt. Das Endergebnis sind validierte Warnungen, die weitere Untersuchungen durch das Sicherheitspersonal erfordern, damit angemessene Reaktionen geplant und ausgeführt werden können.

Von einer verwalteten Priorisierung profitieren Organisationen, die täglich mit einer massiven Anzahl von Warnungen zu kämpfen haben, die die installierten Sicherheitswerkzeuge auslösen. Eine verwaltete Priorisierung wirkt Ermüdungserscheinungen entgegen. Verteidiger können ihre Bemühungen auf höherwertige Untersuchungen konzentrieren. Die personelle Entlastung kann zudem personelle Ressourcen freimachen, die dann im SOC für eine 24/7-Abdeckung eingesetzt werden können.

Verwaltete Priorisierung beantwortet die Frage: Was ist im Moment das Wichtigste?

AUTOMATISCHE PRIORISIERUNG

Priorisierung und Triage sind wiederholbare Prozesse, die oft von SOC-Mitarbeitern ohne Spezialkenntnisse durchgeführt werden und sich gut für eine Automatisierung eignen. Die CrowdStrike Falcon®-Plattform nutzt die Cloud-Analyse zur automatischen Reduzierung von Warnungen, indem zusammenhängende Sicherheitswarnungen überschaubar gruppiert werden. Anschließend wird eine intelligente Priorisierung anhand von Alarmkritizität, Geschwindigkeit und Beziehungen angewandt. So ist sichergestellt, dass kritische Bedrohungen immer im Zentrum der Aufmerksamkeit stehen.

Benutzer der Falcon-Plattform verbringen weniger wertvolle Zeit damit, sich manuell mit harmlosen Warnmeldungen zu befassen. Ihnen bleibt mehr Zeit, sich auf die wichtigen Dinge zu konzentrieren.

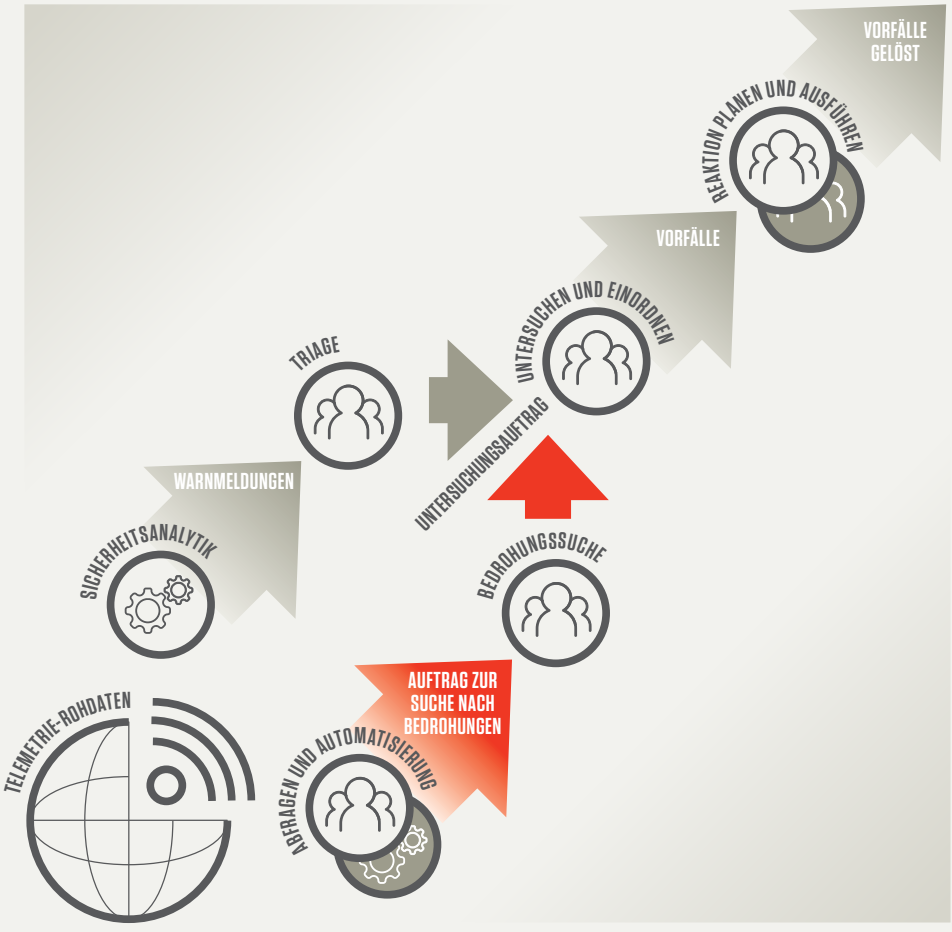
VERWALTETE BEDROHUNGSSUCHE

Ein Service für die verwaltete Bedrohungssuche (Managed Threat Hunting Service) bezieht Menschen in die Gefahrenerkennung ein. Dieser Service nutzt deren umfangreiche Fähigkeiten und Fachkenntnisse, um auch besonders heimtückische Bedrohungen zu erkennen und davor zu warnen.

Angriffe werden letztlich von menschlichen Gegnern ausgeführt, die die Gegenmaßnahmen gut kennen und diesen aktiv ausweichen, um verborgen zu bleiben. Das ist ein Kernproblem der Bedrohungserkennung. Versierte Angreifer werden immer versuchen, automatischen Erkennungstechniken zu entgehen und ihr Vorgehen so zu verschleiern, dass sie wie normale Benutzer erscheinen. Selbstverständlich werden auch automatisierte Erkennungstechniken immer wirksamer werden, aber sie werden Bedrohungen niemals zu 100 % erkennen können. Wer Sicherheitsverletzungen jeder Art stoppen will – auch die besonders raffinierten und komplexen – braucht mehr als nur automatisierte Gegenmaßnahmen.

Die verwaltete Bedrohungssuche beantwortet die Frage: Welche kritischen Bedrohungen sind meinen automatisierten Verteidigungsmechanismen entgangen?

BEDROHUNGSSUCHE ALS TEIL DES ERKENNUNGS- UND REAKTIONSPROZESSES



VERWALTETE BEDROHUNGSSUCHE: DER MENSCHLICHE FAKTOR

Die Bedrohungssuche ist per Definition eine menschliche Tätigkeit und nicht etwas, das sich vollständig automatisieren lässt. Sie deckt ausgefeilte Bedrohungen auf, die gezielt darauf ausgelegt sind, automatisierte Erkennungstechniken der Sicherheitsverantwortlichen zu umgehen. Managed Services, hinter denen kein menschliches Expertenteam für die Bedrohungssuche steht, werden bisweilen als „automatisierte Bedrohungssuche“ bezeichnet.

Doch dabei handelt es sich nicht um eine Bedrohungssuche im eigentlichen Sinn, sondern vielmehr um eine automatische Bedrohungserkennung. Oft arbeiten diese Techniken besonders geräuschvoll in dem Sinne, dass sie laufend Fehlalarme produzieren. Das erzeugt für eine bereits hoch belastete SOC-Organisation einen enormen Arbeitsaufwand.

Doch richtig ausgeführt, erzeugt die Bedrohungssuche eine geringe Anzahl von Sicherheitswarnungen von sehr hoher Qualität. Allerdings setzt sie Fachkenntnisse voraus, damit niedrigschwellige Warnungen nicht überhand nehmen.

Menschliche Angreifer sind listig und kreativ. Zu erwarten, dass man ihre Aktivitäten mit automatisierten Techniken zuverlässig erkennen kann, wäre unrealistisch. Um sie aufzuspüren, bedarf es eines versierten, erfahrenen und kreativen Menschen auf der anderen Seite.

VERWALTETE UNTERSUCHUNG

Lösungsanbieter, die verwaltete Untersuchungen (Managed Investigation) anbieten, verfügen in der Regel über fundiertes Fachwissen und können Unternehmen dabei unterstützen, Bedrohungen schneller einzuordnen. Dabei geht es primär um eine möglichst tiefgehende Analyse des Umfangs und der Schwere eines Vorfalls anhand der zur Verfügung stehenden Daten. Managed Investigations ergänzen Sicherheitswarnungen häufig durch zusätzlichen Kontext, der für ein gründliches Verständnis des Vorfalls erforderlich und für die Planung einer wirksamen Reaktion notwendig ist.

Managed Investigation beantwortet folgende Fragen: Was ist geschehen? Wann ist es geschehen? Wer war betroffen? Wie weit ist der Angreifer gekommen? Und viele weitere.

ANGELEITETE REAKTION

Im Rahmen der angeleiteten Reaktion (Guided Response) erhalten Unternehmen konkrete Empfehlungen zur Eindämmung und Beseitigung einer bestimmten Bedrohung. Dies können Empfehlungen sein, welche Systeme vom Netzwerk isoliert werden sollten oder welche Dateien auf Anzeichen einer Infektion überprüft werden sollten. Ausführlichere Empfehlungen könnten Schritt-für-Schritt-Anweisungen zur Beseitigung einer Bedrohung oder zur Wiederherstellung von Systemen nach einem Angriff umfassen.

Guided Response beantwortet folgende Frage: Was soll ich gegen diese Bedrohung unternehmen?

VERWALTETE PROBLEMBESEITIGUNG

Die verwaltete Problembeseitigung (Managed Remediation) ist der letzte Schritt in der Reaktion auf einen Vorfall: die Wiederherstellung. Ein Managed Remediation Service setzt Systeme wieder auf den Zustand vor dem Angriff zurück, entfernt Malware, säubert die Registry, wirft Eindringlinge heraus und entfernt Persistenzmechanismen. Dieser letzte Schritt ist besonders wichtig und muss unbedingt korrekt ausgeführt werden. Andernfalls wären sämtliche Anstrengungen in den übrigen Phasen des Endgeräteschutzes vergebens. Angreifer verwenden zahlreiche Tricks, um sich festzusetzen, sobald sie in einem Netzwerk Fuß gefasst haben. Geplante Aufgaben, Beobachtungsdienste und redundante Hintertüren sind nur einige Methoden, mit denen sie sich gegen Quarantäne- und Eindämmungsgegenmaßnahmen wappnen.

Managed Remediation beantwortet die Frage: Wie kann ich mein Netzwerk wieder in einen bekannt guten Zustand versetzen und weitere Kompromittierungen verhindern?

Die verwaltete Problembeseitigung (Managed Remediation) ist der letzte Schritt in der Reaktion auf einen Vorfall: die Wiederherstellung. Ein Managed Remediation Service setzt Systeme wieder auf den Zustand vor dem Angriff zurück, entfernt Malware, säubert die Registry, wirft Eindringlinge heraus und entfernt Persistenzmechanismen. Dieser letzte Schritt ist besonders wichtig und muss unbedingt korrekt ausgeführt werden. Andernfalls wären sämtliche Anstrengungen in den übrigen Phasen des Endgeräteschutzes vergebens.

MDR BESCHAFFUNGSLEITFADEN

WELCHER MDR-SERVICE IST FÜR IHRE ORGANISATION DER RICHTIGE?

Unter dem Namen MDR wird eine breite Palette verschiedener Dienstleistungen angeboten. Daher sollten Sie ein klares Bild von den konkreten Fähigkeiten und Anforderungen Ihrer eigenen Organisation haben, damit Sie einen Service wählen, der Ihr Team ergänzt und den größtmöglichen Nutzen bringt. CrowdStrike verfügt über eine Reihe von MDR-Angeboten, die Sicherheitsverantwortliche auf jeder gewünschten Ebene unterstützen.

ALLGEMEINE ÜBERLEGUNGEN

Es gibt einige operative Überlegungen, die für die Wahl eines MDR-Dienstes relevant sind:

Welche Kenntnisse haben Ihre eigenen Fachleute?
Ein Hauptgrund für die Investition in einen MDR-Service ist die gezielte Ergänzung des eigenen Personals um Fachleute, die die Organisation voranbringen und deren Sicherheitsreifegrad steigern, ohne dass Sie teures Personal einstellen müssen.

CrowdStrike ist in der besonderen Lage, erstklassige Experten für die Bedrohungssuche sowie Sicherheitsanalysten aus den verschiedensten Bereichen einzustellen und zu halten, beispielsweise aus Regierungsbehörden, Geheimdiensten, kommerziellen Unternehmen und dem Verteidigungssektor. Mit einer kumulierten Erfahrung von Hunderttausenden von Stunden hat sich das Team von CrowdStrike beim Aufspüren und Stoppen auch komplexester Bedrohungen als effektiv erwiesen.

Hat Ihr Service rechtzeitigen Zugang zu den benötigten Daten und Systemen, um effektiv zu sein?
MDR ist datenintensiv – unabhängig von der spezifischen Ausprägung. Die Effektivität eines bestimmten Dienstes hängt in hohem Maße von der Fähigkeit ab, auf die Daten in der Tiefe und Breite zuzugreifen, die für die Erfüllung seines definierten Auftrags erforderlich sind. Der Zugriff auf die Daten muss in Echtzeit erfolgen, um Bedrohungen schnell erkennen und darauf reagieren zu können.

Die cloud-native Plattform CrowdStrike Falcon für den Endgeräteschutz bietet die ideale Grundlage für MDR. Die Falcon-Plattform sammelt Billionen von Ereignissen pro Woche und deckt dabei Hunderte von verschiedenen Endgeräten ab. Diese Telemetriedaten werden im CrowdStrike Threat Graph® gesammelt, ergänzt, indiziert und analysiert. Threat Graph dient nicht nur als Herzstück der CrowdStrike-Lösungen zum Schutz von Endgeräten, sondern erschließt den MDR-Diensten von CrowdStrike auch den Echtzeit-Zugriff auf die umfangreichen Informationen, die zur Erkennung und Abwehr von Bedrohungen erforderlich sind, sobald diese auftreten.

Wie bleibt Ihr MDR-Team über die neuesten Bedrohungen von Organisationen auf dem Laufenden?
Um neu aufkommende Bedrohungen mit größtmöglicher Wirksamkeit zu erkennen und darauf zu reagieren, müssen Sicherheitsanalytiker unbedingt mit aktuellen Intelligence-Informationen über die neuesten TTPs der aktiven Bedrohungsakteure ausgestattet sein.

Die MDR-Services von CrowdStrike werden mit Daten aus der Bedrohungsaufklärung von CrowdStrike gespeist. CrowdStrike Intelligence bringt Sicherheitsforscher, Kulturkenner und Linguisten zusammen. Das detaillierte, stets aktuelle Wissen über Spionagetechniken von mehr als 130 Gegnern fließt in die Services ein. Diese intime Kenntnis der neuesten verwendeten TTPs stellt bei CrowdStrike eine effektive und effiziente Erkennung und Reaktion sicher.

Wie kommuniziert der MDR-Anbieter mit Ihrem Team?
Alle MDR-Dienste sehen in ihren Workflows zur Aufdeckung, Untersuchung und Beantwortung von Bedrohungen einen Zeitpunkt vor, zu dem das Heft des Handelns an Sie zurückgeht. Im Falle einer reinen Bedrohungssuche ist das dann der Fall, sobald eine validierte Bedrohung entdeckt wird. Im Falle der verwalteten Reaktion liegt dieser Zeitpunkt nach der Eindämmung und Beseitigung der Bedrohung. Die Kommunikation zum Zeitpunkt der Übergabe ist ein potenzieller Reibungspunkt, der die Arbeit Ihres Teams verlangsamen könnte, wenn es sich erst in neue Konsolen, Portale oder Arbeitsabläufe einarbeiten muss.

Für den täglichen Routinebetrieb dient die Konsole von CrowdStrike Falcon als zentrale Kommunikationsdrehscheibe. Sie stellt sicher, dass Sie sofortigen Einblick in alle MDR-Vorgänge innerhalb desselben cloud-basierten Portals haben, das auch für die Wartung und Verwaltung des restlichen CrowdStrike-Lösungspakets verwendet wird. Bei Vorfällen, die nach sofortiger Reaktion des Kunden verlangen, kann die Kommunikation auch per E-Mail oder Telefon erfolgen. So ist stets ein rechtzeitiges Handeln gewährleistet.

Arbeitet Ihr Service rund um die Uhr?
Angreifer nehmen keinen Urlaub. Dasselbe sollte auch für Ihren MDR-Service gelten. Viele Organisationen entscheiden sich auch deshalb für einen MDR-Service, um sich rund um die Uhr gegen Bedrohungen zu schützen, insbesondere wenn das eigene Team nur während der Geschäftszeiten präsent ist.

VERSCHIEDENE MDR-ANGEBOTE ZUR ABDECKUNG IHRER ANFORDERUNGEN

Die MDR-Services von CrowdStrike arbeiten nach dem „Follow-the-Sun"-Modell: Sie erbringen ihre Leistungen 24 Stunden am Tag – sieben Tage die Woche.

Abgesehen von diesen grundsätzlichen Überlegungen berücksichtigt CrowdStrike, dass jede Organisation über bereits vorhandene Fähigkeiten mit Blick auf die Sicherheitsreifekurve verfügt. CrowdStrike hat eine Reihe von MDR-Angeboten, die Organisationen dabei unterstützen, ihre aktuellen Ziele zu erreichen und die 1-10-60-Regel umzusetzen.

PHASE	MDR-AKTIVITÄT	FALCON INSIGHT	FALCON OVERWATCH	FALCON OVERWATCH ELITE	FALCON COMPLETE
Erkennen	Alarmüberwachung, Triage und Priorisierung	✓			✓
	Verwaltete Bedrohungssuche		✓	✓	✓
Untersuchen	Unterstützung bei der erweiterten Untersuchung			✓	✓
Reagieren	Verwaltete Reaktion		✓	✓	✓
	Verwaltete Problembeseitigung: Systeme isolieren				✓
	Verwaltete Problembeseitigung: Persistenzmechanismen beseitigen				✓
	Verwaltete Problembeseitigung: Artefakte entfernen				✓
	Verwaltete Problembeseitigung: Richtlinien abstimmen				✓
Plattform verwalten	Onboarding			✓	✓
	Proaktive Check-ins			✓	✓
	Individuelle Berichte und Briefings			✓	✓
	Agents aktualisieren				✓

Im Folgenden wird eine Reihe von sicherheitsrelevanten Fähigkeiten beschrieben, die je nach den Zielen einer Organisation variieren. Ferner wird die CrowdStrike-Lösung zur Erreichung der jeweiligen Ziele vorgestellt.

ALARMÜBERWACHUNG, TRIAGE UND PRIORISIERUNG

Ziel: Grundlegendes sichtbar machen

Einige Organisationen suchen eine unkomplizierte Plattform für den Endgeräteschutz, mit der sie Bedrohungen automatisch erkennen können und die ihnen eine erweiterte Sichtbarkeit verschafft, ohne dass dies ihre Systeme beeinträchtigt. Bei dem Ziel, Grundlegendes sichtbar zu machen, geht es um die Fähigkeit zur Endgeräteerkennung und Reaktion (EDR), die die Organisation selbst nutzen kann.

Lösung: Falcon Insight

Falcon Insight™ bildet die Grundlage für alle MDR-Angebote von CrowdStrike. Die Falcon-Plattform sammelt Telemetriedaten der Endgeräte, nutzt maschinelles Lernen und Verhaltensanalyse, ergänzt die erhobenen Daten um Kontexte und stellt sie mit leistungsstarken Such- und Abfragefunktionen in Echtzeit zur Verfügung. Diese Funktionalität ist für ein robustes und ausgereiftes SOC erforderlich, damit sich Datendiebstähle und andere Verstöße wirksam unterbinden lassen.

Ziel: Hoher Sicherheitsreifegrad auf Anhieb

Organisationen wollen zwar häufig eine sofortige Reife erreichen, aber ihnen fehlen die Ressourcen, die Erfahrung und die Zeit, um aus eigener Kraft die nötigen Fähigkeiten zur Aufdeckung, Reaktion und Abhilfe zu erwerben.

Lösung: Falcon Complete

Falcon Complete™ stellt auf einzigartige Weise die Technologie, die Plattform, die aussagekräftigen Aufklärungsdaten und das Know-how zur Verfügung – für ein umfassendes Handling und eine durchgängige Endgerätesicherheit. Mit Falcon Complete vertrauen Kunden die Endgerätesicherheit den bewährten Sicherheitsexperten von CrowdStrike an; das gilt für die Implementierung ebenso wie für das Handling und die Reaktion auf Sicherheitsvorfälle. Das Ergebnis ist eine maximierte Sicherheitsaufstellung ohne die Belastung, den Overhead und die Kosten, die für eine erfolgreiche interne Verwaltung der Endgerätesicherheit erforderlich sind. Dahinter steht eine Garantie zur Verhinderung von Datendiebstählen in Höhe von bis zu **1 Million US-Dollar**

BEDROHUNGSSUCHE

Ziel: Unbekannte Bedrohungen erkennen

Einige Organisationen sind potenzielle Ziele für nationalstaatliche oder kriminelle Organisationen, aber sie haben Mühe, das Fachpersonal für ein Rund-um-die-Uhr-Programm zu finden und zu halten, das für die Aufdeckung versierter, gezielter Angriffe auf diesem Niveau erforderlich ist.

Lösung: Falcon OverWatch

Falcon OverWatch ist eine 24/7-Lösung zur verwalteten Bedrohungssuche. Mit OverWatch profitieren Anwender von den branchenweit besten Spezialisten für Sicherheitsabläufe und Bedrohungssuche. Das Team fahndet proaktiv nach ungewöhnlichen oder neuen Aktivitäten von Angreifern und nutzt dabei den CrowdStrike Threat Graph.

Ziel: Sofortige Beseitigung komplexer unbekannter Bedrohungen

Vielen Organisationen fehlen das Fachwissen und die Ressourcen zur Aufdeckung und Beseitigung der gegen sie gerichteten komplexen Bedrohungen.

Lösung: Falcon Complete

Mit Falcon Complete profitieren Kunden von der verwalteten Bedrohungssuche des erfahrenen Teams von Falcon OverWatch. Sobald diese Experten eine Bedrohung finden, arbeiten sie mit dem Team des Kunden zusammen, um den Vorfall zu analysieren, zu untersuchen und zu beheben, bevor aus dem Störfall ein handfester Sicherheitsvorfall wird.

UNTERSTÜTZUNG BEI DER ERWEITERTEN UNTERSUCHUNG

Ziel: Auch unbekannte Bedrohungen gründlich verstehen und einordnen

Organisationen, die bereits ein eigenes Team an Sicherheitsfachleuten beschäftigen, möchten auf externe Ressourcen und Fachkenntnisse zurückgreifen können und somit auch unbekannte Bedrohungen aufdecken.

Lösung: Falcon OverWatch Elite

Falcon OverWatch Elite erweitert die standardmäßige Bedrohungssuche von OverWatch. Ein der Organisation zugewiesener Analyst unterstützt dabei, Bedrohungen zu verstehen, denen die Organisation mit hoher Wahrscheinlichkeit ausgesetzt ist, und sich optimal darauf vorzubereiten, um entsprechend reagieren zu können. Der Analyst führt regelmäßig Audits der Umgebung durch und erweitert die gewonnenen Informationen mit Beobachtungen aus der Community. Zudem übernimmt er Sicherheitsabstimmungen, spricht Empfehlungen zur Falcon-Plattform aus und führt Coachings zu bewährten Praktiken bei Bedrohungssuche und Triage durch. Dadurch ist die Umgebung stets auf maximalen Schutz und Effizienz optimiert, sodass Sie schnell und entschlossen auf neue Bedrohungen reagieren können.

ANGELEITETE REAKTION

Ziel: Klarheit über komplexe Angriffe und Empfehlungen zu Gegenmaßnahmen erhalten

Einige Organisationen suchen die Zusammenarbeit mit Spezialisten für die Bedrohungssuche. Sie erwarten Klarheit zu komplexen Angriffen und Empfehlungen zu notwendigen Gegenmaßnahmen.

Lösung: Falcon OverWatch

Falcon OverWatch sucht in der Umgebung der Organisation proaktiv nach Bedrohungen und weist auf die dringlichsten Bedrohungen hin. In kürzester Zeit werden fundierte Warnmeldungen per E-Mail und über die Management-Konsole der Falcon-Plattform zugestellt. Die Sicherheitsverantwortlichen werden so darüber informiert, wie auf die Bedrohung zu reagieren ist.

Ziel: Empfehlungen und Anleitungen zur Abwehr komplexer Angriffe und zur Problembeseitigung

Einige Organisationen möchten im direkten Dialog mit Spezialisten für die Bedrohungssuche klären, wie die gemeldeten Angriffe am besten abzuwehren oder zu beheben sind.

Lösung: Falcon OverWatch Elite

Falcon OverWatch Elite erweitert die standardmäßige Bedrohungssuche von OverWatch um die Unterstützung eines zugewiesenen Analysten. Der Analyst empfiehlt konkrete Reaktionsmaßnahmen und stellt zudem fundierte Kontexte zu Bedrohungen bereit, die in der Umgebung der Organisation beobachtet wurden.

VERWALTETE PROBLEMBESEITIGUNG

Ziel: Sofortige Abhilfe bei erkannten Bedrohungen rund um die Uhr

Viele Organisationen sehen die Notwendigkeit, effektive und effiziente Abhilfemaßnahmen durchführen zu können, verfügen aber nicht über das nötige Fachwissen oder die Ressourcen.

Lösung: Falcon Complete

Falcon Complete führt alle zur Behebung des Vorfalls erforderlichen Maßnahmen durch. Das Team von Falcon Complete ordnet die Warnmeldung ein, entwickelt eine Strategie zur Beseitigung der Bedrohung unter Einsatz spezifischer Gegenmaßnamen, unterbricht und beseitigt laufende Angriffe, bereinigt kompromittierte Endgeräte und entfernt Malware-Artefakte zur weiteren Analyse.

FAZIT

Die Auswahl der MDR-Dienste ist heutzutage groß. Bei der Suche nach Unterstützung des Sicherheitsteams Ihrer Organisation ist es wichtig, sich zunächst ein fundiertes Bild über dessen Fähigkeiten zur Erkennung, Untersuchung und Reaktion auf Bedrohungen zu verschaffen. Auf dieser Grundlage können Sie einen MDR-Service wählen, der Ihre bestehenden Fähigkeiten ergänzt. Gleichzeitig unternehmen Sie damit wichtige Schritte zur Umsetzung der 1-10-60-Regel.

ÜBER CROWDSTRIKE

CrowdStrike. Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Endgeräteschutzplattform die Sicherheit im Cloud-Zeitalter neu. Die Plattform CrowdStrike Falcon verfügt über eine einzigartige, Cloud-basierte, schlanke Agentenarchitektur, die von künstlicher Intelligenz (KI) unterstützt wird und unternehmensweit für Schutz und Transparenz in Echtzeit sorgt. So werden Angriffe auf Endgeräte sowohl innerhalb als auch außerhalb des Netzwerks verhindert. Mit Hilfe des firmeneigenen CrowdStrike Threat Graph korreliert CrowdStrike Falcon weltweit und in Echtzeit über 2,5 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweitfortschrittlichsten Datenplattformen für Cyber-Sicherheit.

Mit CrowdStrike profitieren Kunden von besserem Schutz, besserer Leistung und sofortiger Time-to-Value – und das alles auf der cloud-nativen Falcon-Plattform.

Über CrowdStrike sollten Sie vor allem eines wissen: Wir stoppen Datendiebstahl.

Testen Sie jetzt kostenlos den Virenschutz der nächsten Generation

Erfahren Sie mehr unter **www.crowdstrike.de**