McAfee MVISION XDR

Die branchenweit einzige proaktive, datensensitive und offene XDR-Lösung

Die Realität bei Sicherheitsabläufen

Das Sicherheitskontrollzentrum (Security Operation Center, SOC) spielt bei der Cyber-Sicherheit von Unternehmen eine zentrale Rolle. Die Hauptaufgabe des SOC besteht darin, Bedrohungen schnellstmöglich aufzuspüren und zu entschärfen, um Schäden an Ressourcen und Daten zu vermeiden. Wenn es im SOC-Getriebe knirscht, gerät die Sicherheit ins Wanken und das gesamte Unternehmen in Gefahr. Die Herausforderungen an das SOC nehmen qualitativ und quantitativ immer weiter zu. Drei Viertel der Sicherheitsspezialisten geben an, dass die Erkennung und Abwehr von Bedrohungen heute schwieriger ist als noch vor zwei Jahren (ESG, 2019). Soll das nun heißen, dass die Gegenseite am Gewinnen ist?

Fairerweise muss darauf hingewiesen werden, dass die SOC-Funktion noch nicht am Ende der Entwicklung angekommen ist: So schätzen 68 % der Unternehmen ihre eigenen Funktionen zur Bedrohungssuche als noch unfertig oder gerade im Aufbau befindlich ein. Und nur 40 % haben laut SANS (2019) die Vorfallreaktion in ihre SOC-Prozesse implementiert.

Nur 26 % berichten, dass ihr SOC bereits einen wichtigen Vorfall erkannt hat.

(Ernst & Young, 2020)

Nur 51 % sind mit der Effektivität ihres SOC bei der Angriffserkennung zufrieden.

(Ponemon Research)

Folgen Sie uns

In den meisten Fällen kommt noch hinzu, dass das SOC unterbesetzt ist. Geeignete Cyber-Sicherheitsexperten sind schwer zu finden und noch schwieriger zu halten. Außerdem wurden SOCs mit einer Vielzahl an isolierten Tools überschwemmt, was die Situation weiter verkompliziert und die schnelle Erkennung von sowie angemessene Reaktion auf Bedrohungen verhindert. Laut ESG Research geben 66 % der Unternehmen an, dass die Wirksamkeit ihrer Bedrohungserkennung und -abwehr eingeschränkt ist, weil sie auf so vielen voneinander unabhängigen Tools basiert.

Für das SOC hat dies zur Folge, dass es Monate dauert, Bedrohungen aufzuspüren und abzuwehren – während die Gegenseite entsprechend mehr Zeit hat, noch mehr Schäden zu verursachen. Erforderlich sind daher Transparenz und Kontrolle über sämtliche Cyber-Ressourcen sowie umsetzbare Daten, um Bedrohungen schnell entschärfen zu können. Die fragmentierten Tools müssen über alle Endgeräte, Netzwerk, Cloud und Anwendungen hinweg integriert und optimiert werden, um Komplexitäten zu beseitigen. Abhilfe gegen die Vielzahl an Warnmeldungen bieten automatisierte Erkennungs- und Analysefunktionen, die Bedrohungen nach Schweregrad einstufen und sortieren. SOCs müssen mit intelligenten und effizienten Erkennungs-, Analyse- und Abwehrfunktionen ausgestattet werden, um Angriffen zuvorzukommen oder diese zumindest zu entschärfen, bevor ernste Schäden eintreten.

Behebung von Ineffizienzen im SOC

McAfee® MVISION XDR ist die Antwort auf all diese Herausforderungen und operativen Unzulänglichkeiten beim SOC. Nur diese Lösung dehnt die erweiterten Erkennungs- und Reaktionsfunktionen (XDR) als Cloud-basierte hochentwickelte Bedrohungsverwaltung auf die gesamte IT-Infrastruktur aus, indem sie den kompletten Lebenszyklus von Angriffen abdeckt, beim Schutz zwischen den wichtigsten Daten unterscheidet und es ermöglicht, mit einfachen Schritten eine wirksame Reaktion zu koordinieren. MVISION XDR verringert Risiken vom Endgerät bis zur Cloud und steigert innerhalb kürzester Zeit die Effektivität des SOC. Die erste offene, proaktive und datensensitive XDR-Lösung verkürzt die Reaktionszyklen und spart dabei noch 95 % der Kosten[1] für die Beurteilung von Bedrohungskampagnen ein.

Dank des zentralen Überblicks über Endgeräte, Netzwerk und Cloud hinweg bieten sich SOCs ganz neue Möglichkeiten. MVISION XDR bietet folgende Vorteile:

- Hilft bei der Vermeidung manueller Fehler, die durch den ständigen Wechsel zwischen Tools und Daten verursacht werden.
- Schützt die wichtigsten Daten und unterscheidet dabei fein abgestuft nach Schweregrad und Vertraulichkeit.
- Minimiert die Risiken mit präventiven Analysen, geführten und automatisierten Untersuchungen sowie empfohlenen Gegenmaßnahmen – sowohl vor als auch nach Angriffen.
- Verbessert die Transparenz und Kontrolle und macht aufwändige manuelle Aufgaben überflüssig, indem Sicherheitslösungen mühelos für die Zusammenarbeit koordiniert werden.
- Legt die Verwaltung der Cyber-Sicherheit in die Hände des vorhandenen Personals, ohne dass neue Mitarbeiter erforderlich werden.

Mehr als 4 Millionen Stellen sind unbesetzt, 65 % der Unternehmen berichten von einem Engpass bei Cyber-Sicherheitsexperten, und 61 % der Bewerber sind nicht qualifiziert.

(ISC2)

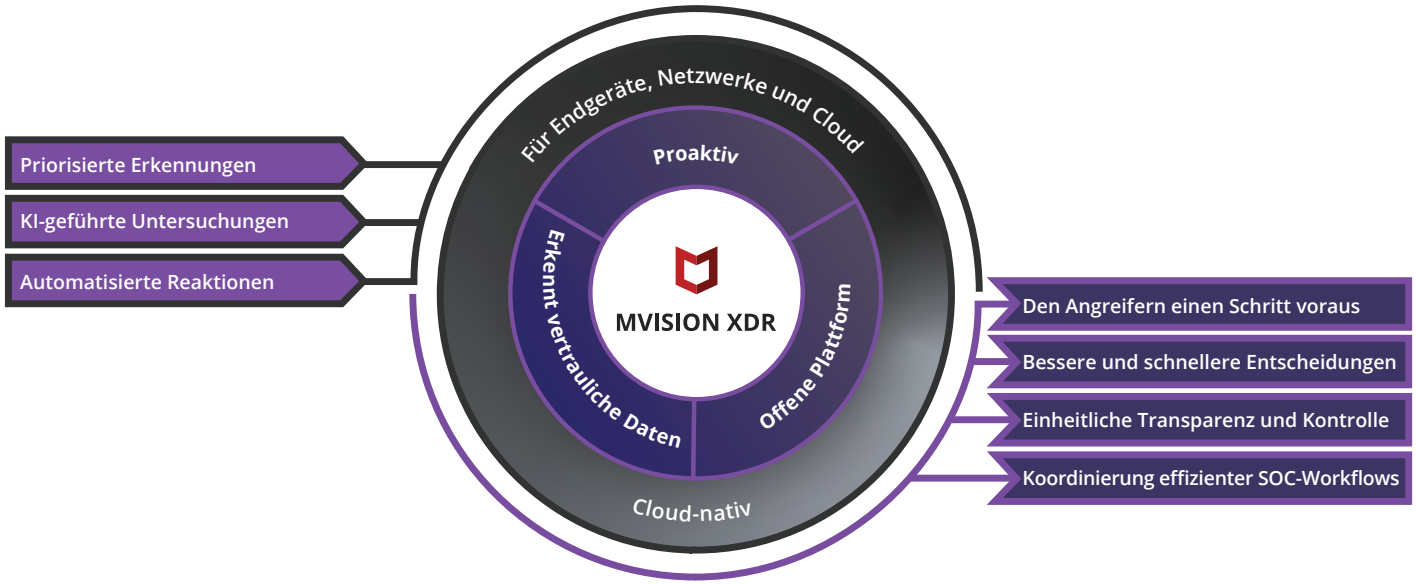

Abbildung 1. Die Vorteile von MVISION XDR.

Handfester Vorsprung mit proaktiven Analysen

Die meisten XDR-Lösungen können erst etwas ausrichten, nachdem ein Angreifer in die Umgebung eines Unternehmens eingedrungen ist. Das führt zu reaktiven SOCs, die sich permanent mit dem Ernstfall konfrontiert sehen. MVISION XDR ist – zusammen mit McAfee® MVISION Insights – die einzige XDR-Lösung, die den gesamten Lebenszyklus von Angriffen abdeckt.

Neue proaktive Funktionen stehen bereit, bevor ein Angriff stattfindet, und stärkere reaktive Workflows übernehmen nach dem Angriff. So können es SOCs mit externen Bedrohungen aufnehmen, die wirklich relevant sind, und noch bevor ein Angriff stattfindet. Unternehmen können Bedrohungen priorisieren, die Effektivität von Gegenmaßnahmen vorab einschätzen und Abhilfemaßnahmen vorgeben. Das Ergebnis ist eine schnellere Erkennung und Reaktion, die innerhalb von Minuten anstatt von Wochen erfolgt.

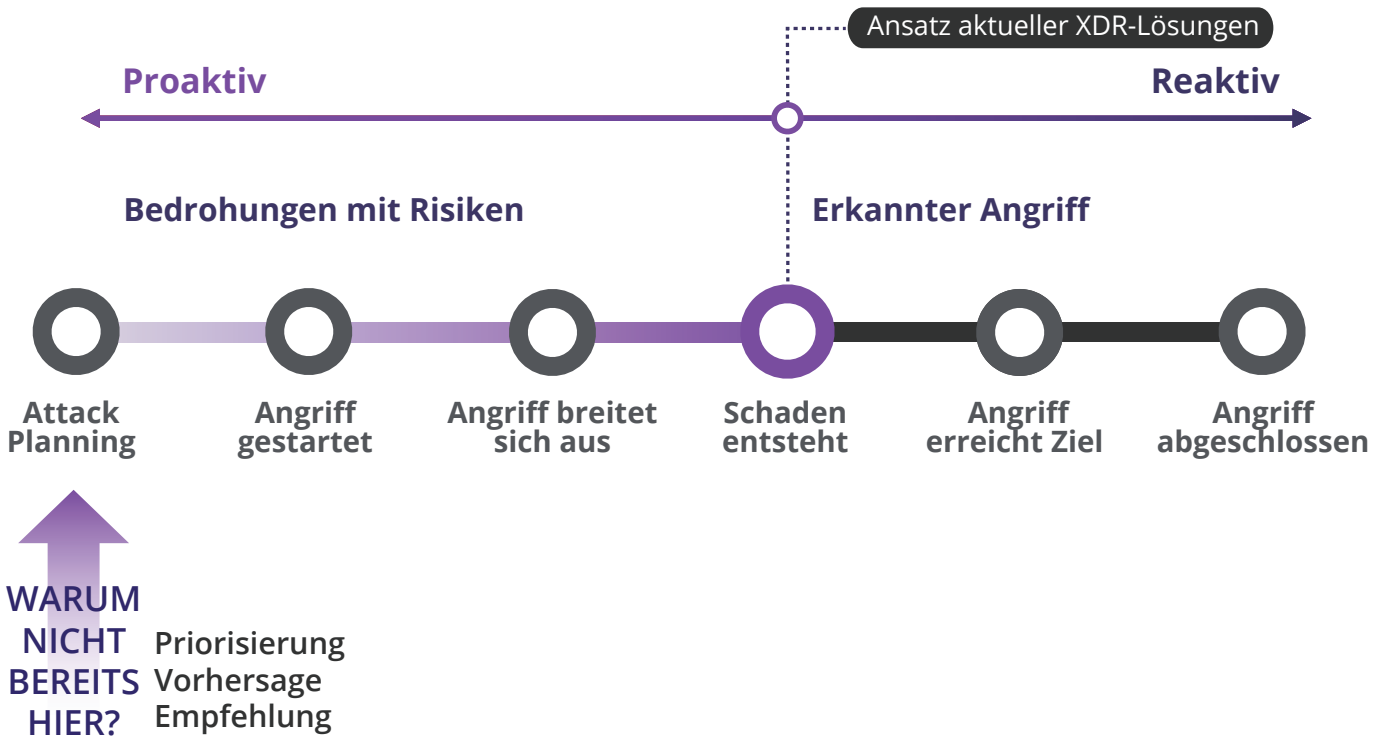

Abbildung 2. MVISION XDR deckt den gesamten Lebenszyklus von Cyber-Angriffen ab.

Einheitliche Transparenz und Kontrolle für mehrere Vektoren

Die Aktivitäten und Winkelzüge von Angreifern über die verschiedensten Vektoren hinweg sind oftmals schwer zu deuten. Daher benötigen Sie dringend eine Möglichkeit, die Warnsignale zu deuten und das Puzzle zusammenzusetzen. Noch wichtiger ist jedoch, dass Analysten in der Lage sein müssen, bei erkannten Bedrohungen vektorübergreifend einschreiten zu können. MVISION XDR fasst die Telemetrie von Cloud- und lokalen Sensornetzwerken zusammen, um nahtlos einen ganzheitlichen Überblick über Unternehmensdaten zusammen mit verdächtigen Verhaltensmustern bereitzustellen. Durch das Zusammenfassen endloser Ströme von Warnmeldungen aus dem ganzen Unternehmen zu einer kleineren Anzahl von Vorfällen filtert MVISION XDR die wichtigsten Informationen heraus und führt Analysten näher an eine Lösung heran.

Ein intuitives Dashboard zeigt SOC-Analysten die wichtigsten Erkenntnisse aus ihrer Umgebung, gibt Aufschluss über aktive Kampagnen und gibt Empfehlungen zu Prioritäten, die auf automatisierten Untersuchungen und Analysen basieren.

Diese Übersicht können Analysten weiter aufschlüsseln, verdächtige Punkte näher untersuchen und erforderliche Maßnahmen abschätzen. Die möglichen Gegenmaßnahmen können die verschiedensten Vektoren im gesamten Unternehmen betreffen.

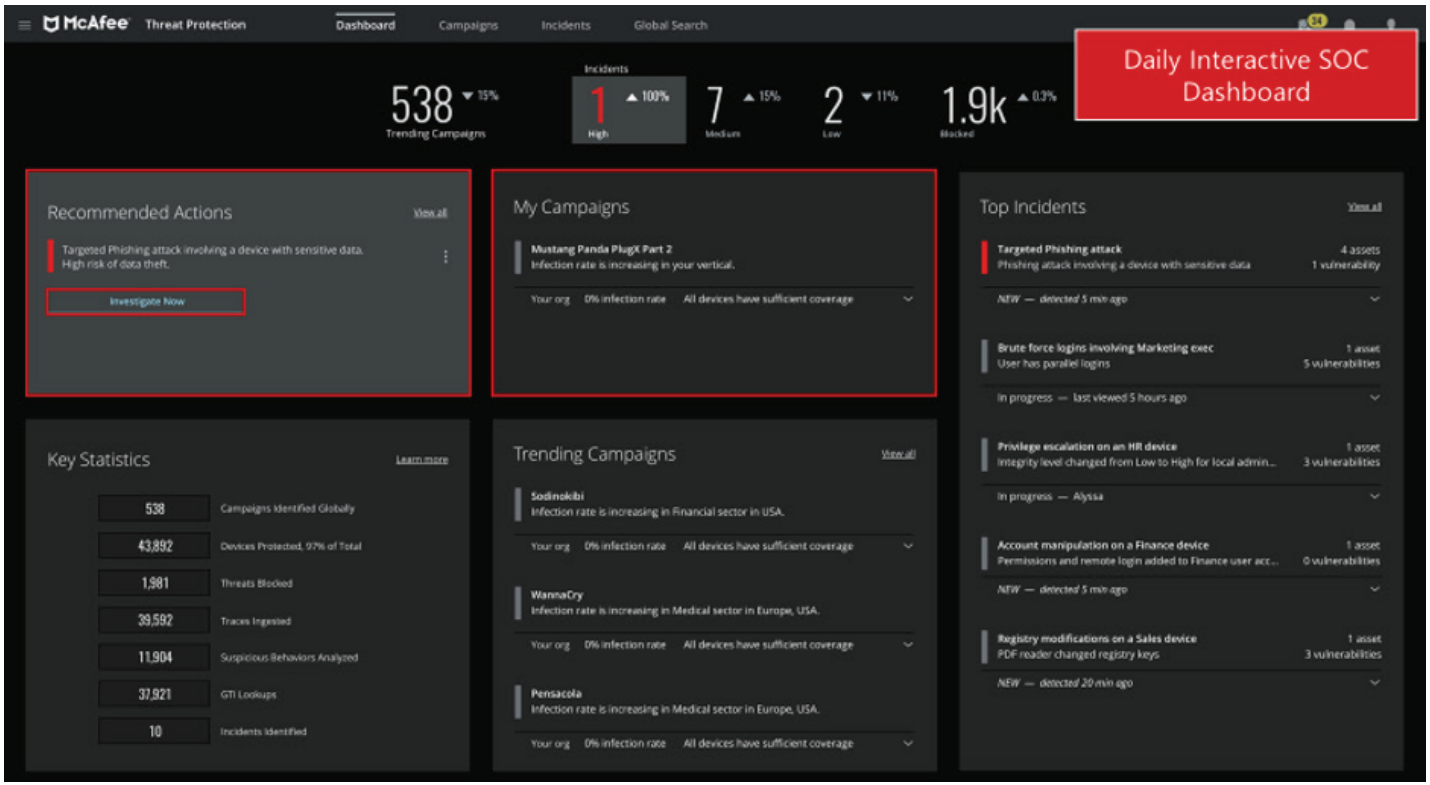

Abbildung 3. Das intuitive und interaktive Dashboard von MVISION XDR.

Bessere und schnellere Entscheidungen

SOCs müssen Entscheidungen schnell treffen, um Bedrohungen zu entschärfen und Schäden zu minimieren. Dazu ist es notwendig, Untersuchungen zu beschleunigen und Befunde nach ihrem Schweregrad zu priorisieren. MVISION XDR erreicht dies mit KI-geführten bzw. automatischen Untersuchungen. KI-geführte Untersuchungen leiten SOC-Analysten mithilfe automatischer Fragen und Antworten durch die Erfassung, Zusammenfassung und Visualisierung von Beweisen aus mehreren Quellen. Dies hilft SOC-Analysten, kontinuierlich zu lernen, während sie ihre Untersuchungen und Gegenmaßnahmen immer weiter perfektionieren. Außerdem können auch jederzeit automatische Untersuchungen durchgeführt werden, die von bewährten Priorisierungslogiken von Bedrohungen abgeleitet sind. Beide Optionen machen das manuelle Sammeln und Analysieren von Beweisen überflüssig. Außerdem reduzieren sie den ständigen Strom an Warnmeldungen auf das Wesentliche und geben Analysten die Möglichkeit, umgehend über Gegenmaßnahmen zu entscheiden.

Abbildung 4. Von MVISION XDR festgestellte Vorfälle, die ein Risiko für vertrauliche Daten darstellen, und deren zeitlicher Verlauf.

MVISION XDR erfasst Bedrohungsdaten aus einer Vielzahl von Quellen, z. B. aus SIEM-Lösungen (Sicherheitsinformations- und Ereignis-Management). Außerdem sind bequeme Suchmöglichkeiten nach Verantwortlichen oder Quelle eines Vorfalls bzw. einer Bedrohung vorhanden. Auf einer Zeitleiste wird übersichtlich gezeigt, was geschehen ist und was genau ein Angreifer damit beabsichtigt hat – zusammen mit den zugehörigen Daten und Verhaltensmustern. Analysten können diese Erkenntnisse und Beweise weiter aufschlüsseln, um den Zwischenfall anhand ihrer eigenen Kenntnisse und Intuition genauer einzuschätzen. Die Lösung empfiehlt Aktionen basierend darauf, welche Gegenmaßnahmen zu einem früheren Zeitpunkt im Unternehmen getroffen wurden oder wie andere Branchenvertreter reagiert haben.

MVISION XDR stellt eine Auswahl von Priorisierungen bereit, damit Sie schnellstmöglich wichtige Entscheidungen treffen können. Bedrohungen und Vorfälle können anhand der Folgen für das Unternehmen (z. B. Datenverlust oder Schäden) priorisiert werden. Eine Bedrohung, die bestimmte Kriterien in Bezug auf Datenschutz, Identität oder Gerätetyp erfüllt, kann mit einer höheren Priorität eingestuft werden. So hätte zum Beispiel ein Gerät, auf dem ein hochrangiger Finanzmanager hochvertrauliche Daten speichert, im Falle einer Bedrohung Vorrang.

Mühelose Koordinierung effizienter SOC-Workflows

MVISION XDR ist eine offene, integrierte Plattform, die über viele Vektoren skaliert und andere Sicherheitsfunktionen miteinander verbindet. Dadurch können andere Sicherheitstools koordiniert agieren und Angreifer abwehren. Da der Benutzer nicht mehr manuell zwischen den verschiedenen Tools wechseln und Daten per Kopieren und Einfügen übertragen muss, wird Zeit gespart und das Fehlerpotential gesenkt. Außerdem können so auch Erkennungen aus verschiedenen Sicherheitstools genauer zugeordnet werden, was die Verlässlichkeit von Warnungen erhöht und bessere Entscheidungen ermöglicht. Dank der offenen API (Application Programming Interface) können Unternehmen eigene Workflows (z. B. für die Suche, Untersuchung, Reaktion oder Gegenmaßnahmen) mit Lösungen von McAfee bzw. Drittanbietern aus dem benutzerfreundlichen Marktplatz leicht erstellen und so die Abwehr von Cyber-Bedrohungen optimieren.

Beispiele für andere Lösungen von Drittanbietern wären IT-Ticketerstellung, SOAR (Security Orchestration Automation Response, Sicherheitsorchestrierung, Automatisierung und Reaktion), SIEM und Bedrohungsdaten. Dank MVISION XDR können Sie vorhandene Investitionen weiter nutzen – unabhängig davon, ob diese von McAfee oder von Drittanbietern stammen. Es besteht kein Grund, Ihre aktuellen Cyber-Sicherheitsmaßnahmen auszutauschen.

Mit MVISION XDR können Sie die Funktionen und Workflows ganz nach Ihrem eigenen Zeitplan implementieren. Das Engagement von McAfee für offene, integrierte Sicherheit, die das Weitergeben von Informationen und Koordinieren von Schutzmaßnahmen vereinfacht, zeigt sich auch in unserer Rolle als Mitbegründer der branchenweiten Sicherheitsinitiative Open Cyber Security Alliance (OCA). Außerdem sind wir an der OpenDXL-Ontologie beteiligt, einem allgemeinen Übertragungsmechanismus und Protokoll für den Informationsaustausch.

Mit MVISION XDR, der einzigen proaktiven, datensensitiven und offenen XDR-Lösung, kann das SOC Bedrohungen schnell und zuverlässig erkennen, angehen und abwehren. SOCs können Auslöser schnell durchsehen und Vorfälle sowie Ursachen analysieren, um Bedrohungen zu beheben und proaktiv Schutzmaßnahmen gegen die gefährlichsten Bedrohungen zu ergreifen.

1. Interne Kundenrecherche von McAfee.

Dieses Dokument enthält Informationen zu in der Entwicklung befindlichen Produkten, Services bzw. Prozessen. Für die hier beschriebenen Vorteile muss das System entsprechend konfiguriert werden, und es müssen Hard- bzw. Software oder Services aktiviert werden. Die hier bereitgestellten Informationen können ohne Vorankündigung und nach alleinigem Ermessen von McAfee geändert werden. Wenden Sie sich an Ihren McAfee-Vertreter, um die neuesten Prognosen, Zeitpläne, Spezifikationen und Roadmaps zu erhalten.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de