McAfee MVISION Insights

Die erste Endgerätelösung mit erweiterten Erkennungs- und Reaktionsfunktionen (XDR), damit Sie Ihren Angreifern stets einen Schritt voraus bleiben

Die Evolution und Geschwindigkeit von Cyber-Bedrohungen ist eine ständige Gefahr für Unternehmen. Vor dem Hintergrund des IT-Fachkräftemangels erhöhen diese ihre Sicherheitsbudgets, können aber dennoch nicht mit fortschrittlichen Angreifern Schritt halten, die ständig an ihrem Arsenal aus Tools, Taktiken und Techniken arbeiten. Aktuell sind isolierte Bedrohungsdaten verfügbar, mit denen sich durch menschliches und manuelles Eingreifen unmittelbare Bedrohungen beheben lassen. Die zunehmende Zahl und Raffinesse von Cyber-Angriffen führt jedoch dazu, dass Sicherheitsteams praktisch nur noch reaktiv agieren können. Eine Plattform für Bedrohungsdaten kann eine große Datenbank für Informationen zu Bedrohungen bereitstellen, erfordert jedoch manuelle Integration und die Arbeit von Analysten. Das wiederum hat zur Folge, dass Nutzbarkeit und Behebungsmöglichkeiten eingeschränkt bleiben. Die Schwachstellenverwaltung kann zwar Empfehlungen zu bestehenden Schwachstellen und ihrem Schweregrad geben, bietet jedoch nur wenig Einblick dazu, ob und wie Ihre Sicherheitsaufstellung reale und aktuelle Bedrohungen abwehren kann.

Die Lösung dieses Dilemmas ist McAfee® MVISION Insights mit Echtzeit-Bedrohungsdaten, die proaktive Aktionen ermöglichen. Umfassende Bedrohungsdaten, die von künstlicher Intelligenz sowie menschlichen Sicherheitsexperten aufbereitet und analysiert wurden, erlauben die Priorisierung der Bedrohungen und Kampagnen, die Ihr Unternehmen am wahrscheinlichsten betreffen werden. McAfee MVISION Insights sagt präzise die Auswirkungen einer Bedrohung auf Ihre Gesamtsicherheit voraus und gibt genaue Empfehlungen dazu, wie Sie Ihre Sicherheitsaufstellung optimieren können.

Hauptvorteile

- **Von einer Milliarde Sensoren erfasste Risiko-Bedrohungsdaten:** Identifizieren Sie Bedrohungen proaktiv außerhalb Ihrer Unternehmensperipherie durch eine vertrauenswürdige Quelle. Priorisieren Sie Bedrohungen basierend auf Branche, Region, Bedrohungsakteuren und Endgeräte-Sicherheitsaufstellung Ihres Unternehmens.
- **Identifizierung von Bedrohungskampagnen vor einem Angriff und Priorisierung Ihrer Risikostufe in einer zentralen Konsole:** Sie erhalten umsetzbare Informationen zu einer Bedrohung und dazu, wie Ihre Endgerätesicherheit dagegen aufgestellt ist, sowie Empfehlungen zur Behebung.
- **Verkürzung der Zeit von der Erkennung bis zur Behebung:** Optimieren Sie Workflows, um zusätzliche Sicherheitsmaßnahmen zu beschleunigen. Sie erhalten praktische Informationen zu erforderlichen Änderungen zur Verbesserung Ihrer Endgeräte- und Cloud-Sicherheitslage und können die Reaktionszeit von Monaten auf Stunden verkürzen.

Folgen Sie uns

Wechsel zu proaktiver Sicherheit

MVISION Insights stellt Funktionen für die McAfee®-Verwaltungsplattform bereit, mit denen Abläufe zur Risiko- und Bedrohungsabwehr eingebunden und optimiert werden, um mit weniger Ressourcen defensive Gegenmaßnahmen präventiv zu verstärken und die Reaktionszeit zu verkürzen. Die von Milliarden Sensoren abgerufenen und optimierten Risikodaten, die von erfahrenen Bedrohungsforschern analysiert werden, geben Ihrem Unternehmen die notwendigen Einblicke, um Ihre Schutzfunktionen zu priorisieren. In der zentralen Konsole kontrollieren Sie die Erkennungs- und Behebungsmaßnahmen, beschleunigen präventiv die Reaktionszeiten und können so die Risiken erheblich verringern.

Reaktive Cyber-Sicherheitsstrategien spielen eine wichtige Rolle als Cyber-Sicherheitskomponente, müssen jedoch nicht bedeuten, dass Ihr Unternehmen den Angreifern stets einen Schritt hinterher läuft und darauf beschränkt ist, Brandherde zu löschen. Ihre Gegenspieler nutzen hochmoderne Tools, mit denen sie Kampagnen gegen herkömmliche Schutzmaßnahmen entwickeln, und testen reaktive Sicherheitsprodukte darauf, welche Techniken Erfolg versprechen. Unternehmen müssen den gesamten Angriffszyklus vor und nach der Attacke abdecken.

Vollständiger Überblick über den Angriffszyklus

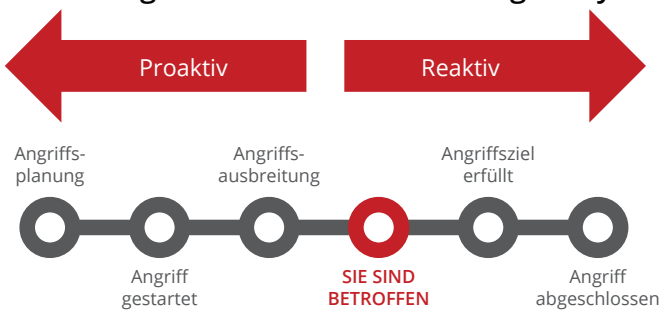

Abbildung 1. Ein typischer Angriffszyklus.

Im Endeffekt ermöglichen Bedrohungsdaten und umsetzbare Erkenntnisse die bestmögliche Cyber-Sicherheitsaufstellung gegen die wahrscheinlichsten Bedrohungen und steigern das Vertrauen in Ihre Schutzmaßnahmen. McAfee MVISION Insights erreicht das wie folgt:

- **Automatische Identifizierung noch unbekannter weltweiter Bedrohungen:** MVISION Insights greift auf einen gewaltigen Bestand an Sicherheitsdaten von über einer Milliarde Sensoren zu, die gemeinsam von Mensch und Maschine für optimierte Bedrohungsanalysen genutzt werden. Mit Machine Learning werden bislang unbekannte Bedrohungen entdeckt, die menschlichen Analysten aufgrund fehlender Visualisierung und Verarbeitung entgehen würden. Gleichzeitig können die Menschen mit ihrer Intuition und Erfahrung die Kniffe und den Einfallsreichtum der menschlichen Angreifer hinter dem Code erkennen.
- **Besserer Überblick über die Sicherheitslage und Konzentration auf Wichtiges:** Sie erfahren exakt, wie Ihre Sicherheitsmaßnahmen aufgestellt sind, bevor die Bedrohungen zuschlagen können. MVISION Insights überwacht und priorisiert lokale und globale Bedrohungen, die Ihr Unternehmen voraussichtlich treffen werden.
- **Machine Learning-Analysen:** Diese Funktion liefert mithilfe von Erfassungspunkten auf Endgeräten und der Cloud wichtige Hinweise dazu, wie Ihre konkrete umfassende Sicherheitsaufstellung abschneiden würde, und empfiehlt dann präventiv entsprechende Schutzmaßnahmen, die sich schnell und einfach implementieren lassen.

MVISION Insights bietet Antworten auf Fragen zum Risiko – für Endgeräte und darüber hinaus

- Sind Sie gefährdet? Wie hoch ist Ihr Gefährdungsgrad?
- Wie priorisieren Sie die Angriffe, die Ihr Unternehmen treffen könnten? Wie haben Sie davon erfahren? Welche Untersuchungsmethode nutzen Sie?
- Woher wissen Sie, welche Bedrohungen Ihr Unternehmen wahrscheinlich treffen werden?
- Selbst wenn Sie eine Plattform für Bedrohungsdaten nutzen, wie können Sie in deren Datenbank die Angriffe priorisieren?
- Wie erfahren Sie von Bedrohungen, die Ihre Kollegen treffen?
- Wie häufig ist das in Ihrer Branche und Region?
- Wird mein Unternehmen von einem konkreten Bedrohungsakteur angegriffen?
- Wie kann Ihre aktuelle Sicherheitsaufstellung diese Bedrohung eindämmen?
- Welchen Überblick haben Sie über die komplette Bedrohungslage und warum?

MVISION Insights-Dashboard für proaktive Sicherheit

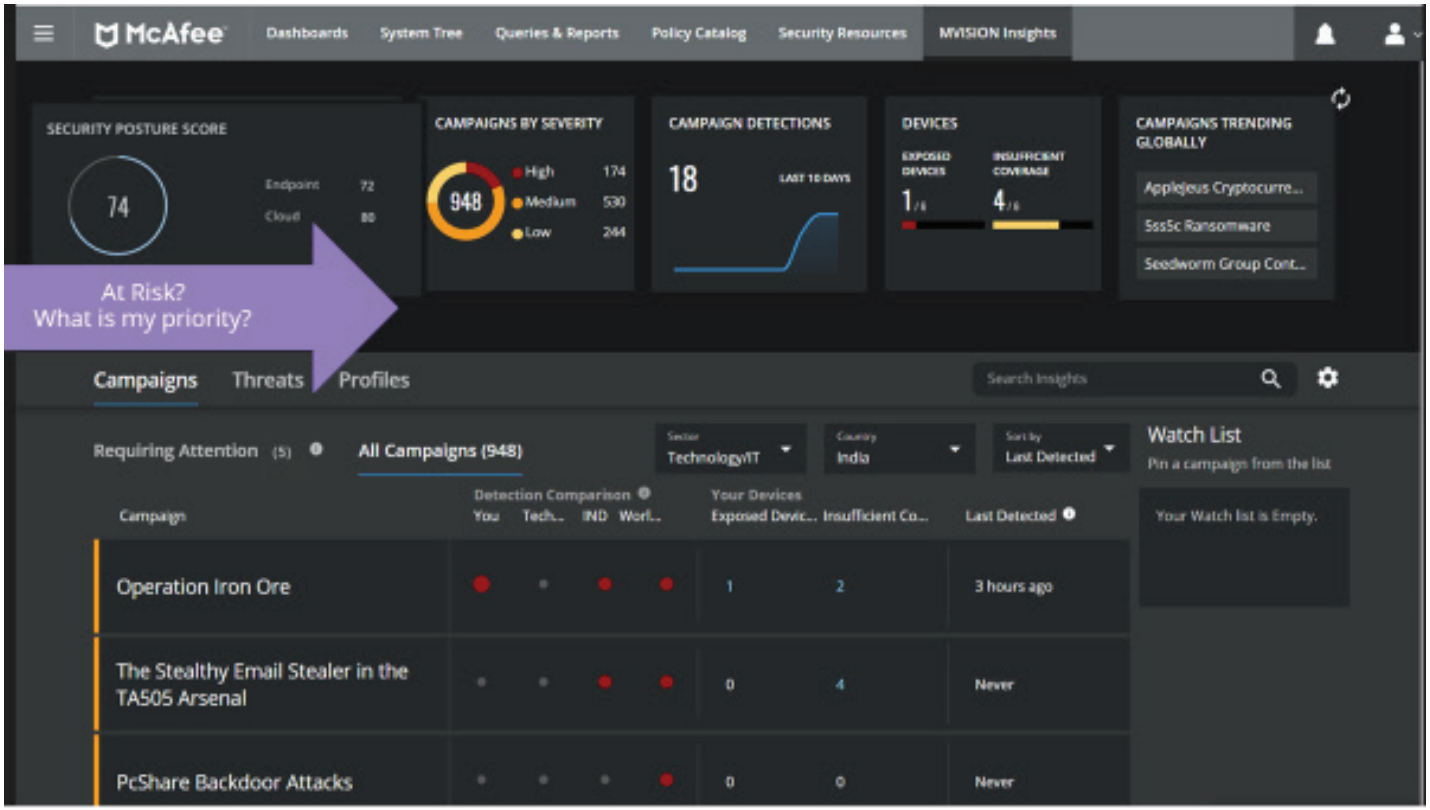

Abbildung 2. Dashboard von MVISION Insights.

Verbesserter Schutz dank Überblick über die komplette Sicherheitsaufstellung

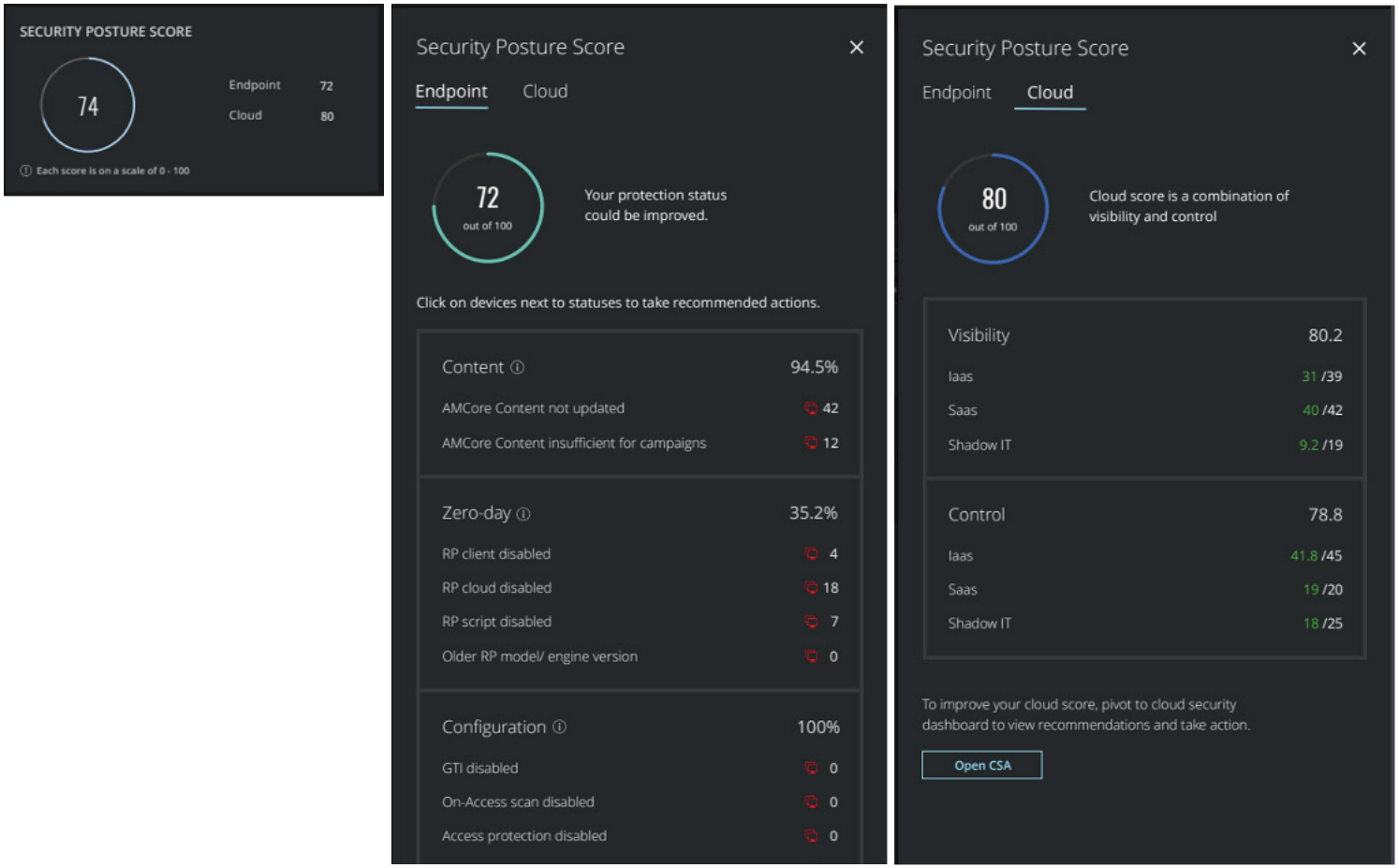

Abbildung 3. Einheitlicher und sofort nutzbarer Überblick über die Sicherheitslage.

Nutzbare Risikobewertungen

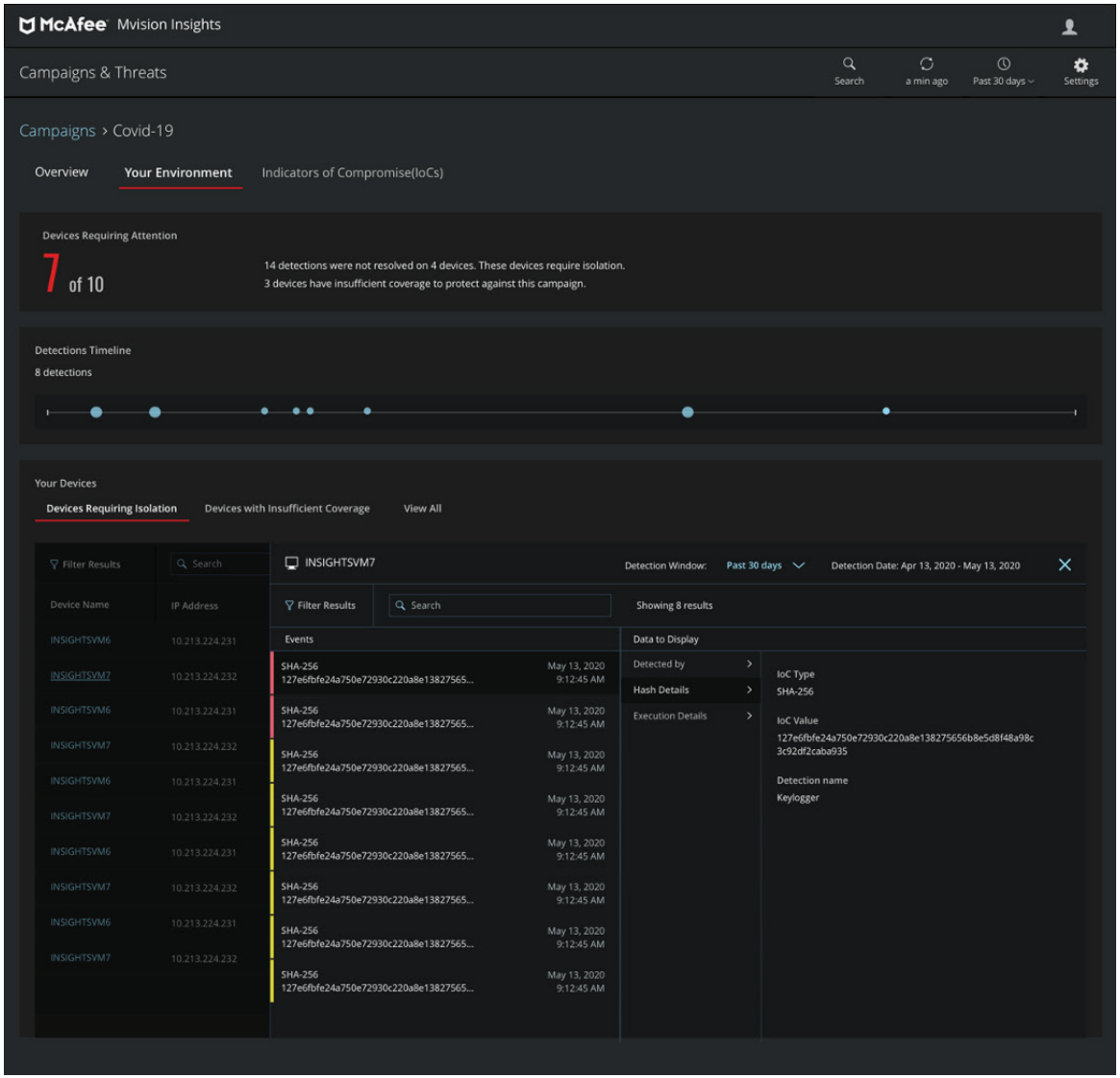

Abbildung 4. Nur wenn Sie wissen, was in Ihrer Umgebung Ihre Aufmerksamkeit erfordert, können Sie die Bedrohung proaktiv abwehren.

Erheblich beschleunigte Erkennung und Reaktion

Mit MVISION Insights geht Ihr Unternehmen den nächsten wichtigen proaktiven Schritt zur Änderung und Wiederherstellung Ihrer individuellen Umgebung mit Empfehlungen und automatisierten Aktionen. Mithilfe von Automatisierung wird die Wirksamkeit der Abwehr externer Angriffe gesteigert. Dazu werden externe Bedrohungen automatisch analysiert und verglichen sowie entsprechende proaktive Schutzmaßnahmen noch vor dem Angriff implementiert.

- **Verkürzung der mittleren Erkennungs- und Behebungszeit von Monaten auf Minuten:** Durch Zusammenarbeit von Mensch und Maschine (Deep Learning, Machine Learning) werden die Möglichkeiten hochentwickelter Analysefunktionen erweitert, sodass enorme Datenmengen durchsucht und aktuelle, umsetzbare Erkenntnisse präsentiert werden können. Mithilfe erweiterter Erkennungsfunktionen lassen sich die Reaktionszeiten präventiv verkürzen, wodurch das Risiko erheblich verringert wird.
- **Verbesserung der Qualität von Bedrohungsindikatoren:** Durch erweiterte Analysen können Sie mehr Ereignisse erkennen und die Warnmeldungen besser interpretieren. Bei der Bedrohungsanalyse in MVISION Insights können Sie mühelos zu McAfee® MVISION EDR wechseln, um nach weiteren Kompromittierungsindikatoren zu suchen und die Zahl der Untersuchungszyklen zu verringern. Wichtiger Kontext zu Bedrohungsakteuren und kriminellen Organisationen hinter der Kampagne wird weitergegeben: die verwendeten Tools, die ihnen zugeordneten typischen Schwachstellen (Common Vulnerabilities and Exposures, CVEs), ihre standardmäßigen Taktiken und Methoden sowie zugehörige Kompromittierungsindikatoren, aber auch vertrauenswürdige Quellen zu Informationen über die Akteure und Gruppen.
- **Bedrohungen werden auf verständliche Weise präsentiert, wobei die Informationen priorisiert sind und sich verwerten lassen.** Ein umfassender und einheitlicher Sicherheitsansatz umfasst Endgeräte- sowie Cloud-Analysen, damit Sie Zeit für wichtige Aufgaben in Ihrer Umgebung haben. Die Empfehlungen für Reaktionen basieren auf analysierten und priorisierten Bedrohungsdaten und Einblicken, sodass selbst unerfahrene Analysten zuverlässige Analysen durchführen können. In der integrierten Konsole können Sie schnell und einfach reagieren – Änderungen an Ihren Konfigurationen vornehmen, infizierte Geräte isolieren, Richtlinien aktualisieren oder zu Lösungen für Erkennungs- und Reaktionsmöglichkeiten für Endgeräte (EDR) wechseln.

Unterstützung für SOC-Mitarbeiter

Sicherheitsteams sind von der schieren Flut an Informationen überwältigt, die sie zum Schutz ihrer Umgebungen durchsuchen müssen. Eingeschränkte Ressourcen und knappe Zeit erschweren Bedrohungsanalysen sowie Schutzmaßnahmen. Durch die Zusammenarbeit von Mensch und Maschine werden Analysemöglichkeiten unabhängig von den Kompetenzen der Analysten erweitert, um enorme Datenmengen durchsuchen und diese als umsetzbare Informationen bereitstellen zu können. MVISION Insights ermöglicht Ihrem Unternehmen die Schließung der Kompetenzlücke und Stärkung der SOC-Mitarbeiter. Sicherheitsteams sind besser informiert und können somit auch bessere Entscheidungen treffen.

- Sicherheitsteams können aus den Überwachungsdaten zusätzliche Erkenntnisse ziehen, mit denen sie die Abwehrmaßnahmen Ihres Unternehmen anpassen und optimieren und so maximalen Schutz bieten können – ohne dass zusätzliche Mitarbeiter oder höhere Kompetenzen benötigt werden. MVISION Insights bietet wichtige Einblicke in MVISION EDR, um die Länge des Untersuchungszyklus verkürzen. Damit erhalten Analysten die für Untersuchungen notwendige Expertise und Ressourcen, sodass sie das Risiko des Zwischenfalls sowie die Ursache des Problems schneller und effizienter überprüfen können.
- CSOs (Chief Security Officer) können ihre vorhandenen Mitarbeiter und Lösungen optimal einsetzen, da erfahrene Sicherheitsanalysten von einfachen Aufgaben entlastet werden und noch unerfahrene Mitarbeiter effektiver arbeiten können. Dadurch reduziert sich der Zeitaufwand für die Sicherheitsverwaltung. Mit optimierten Workflows lassen sich zusätzliche Sicherheitsmaßnahmen beschleunigen.
- Erkennung, Reaktion und Schutzmaßnahmen werden in einer zentralen Konsole präventiv automatisiert, sodass Analysten nicht mehr zwischen verschiedenen Aufgaben wechseln müssen. MVISION Insights erfasst sowie analysiert relevante Datenelemente zentral und verbindet sie mit relevanten Empfehlungen, die Sicherheitsanalysten bei Bedarf sofort umsetzen können.

Umfangreichere Einblicke

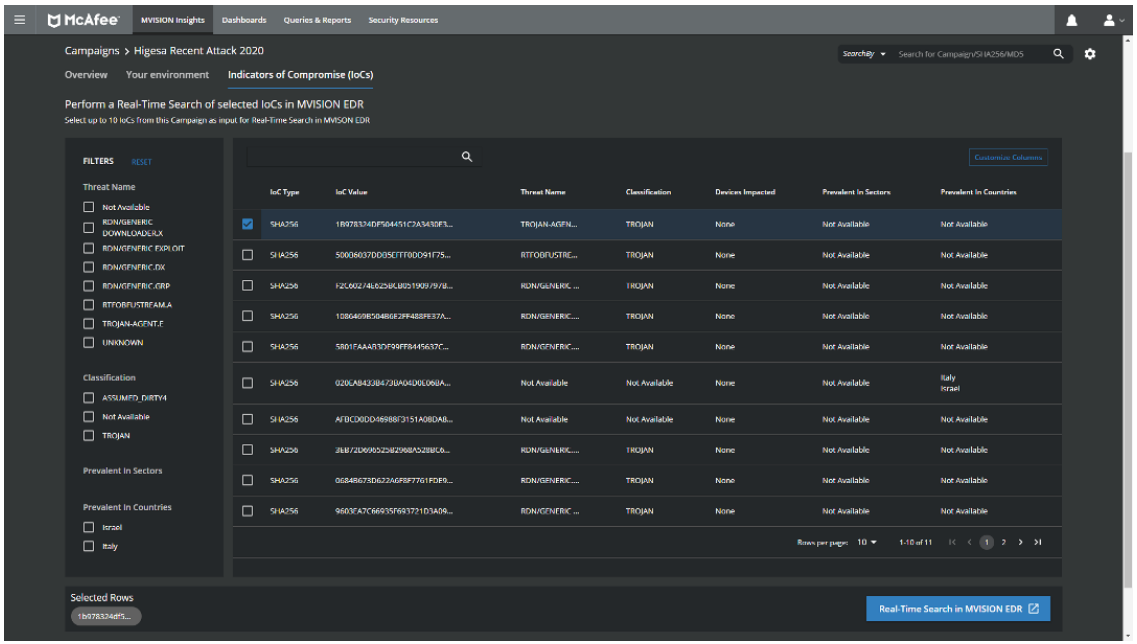

Abbildung 5. Dank umfassender Informationen und EDR-Funktionen können Sie Bedrohungsereignisse verstehen und feststellen, ob Sie Ihr Unternehmen zuverlässig schützen können.

Anforderungen von MVISION Insights

MVISION Insights wird per McAfee® ePolicy Orchestrator® (McAfee® ePO™) 5.10 (lokal und IaaS) sowie McAfee® MVISION ePO™ (SaaS) verwaltet. Die Lösung wurde für die Zusammenarbeit mit unserer neuesten Endgeräteschutz-Technologie optimiert: McAfee® Endpoint Security und McAfee® Agent. Damit MVISION Insights effektiv funktioniert, muss die Erfassung und Übertragung von Telemetriedaten in McAfee Endpoint Security aktiviert werden.

Anwendungsbeispiele

Problem	Lösung	Ergebnis
Werde ich angegriffen? **Ist das eine neue Kampagnenvariante?**	▪ Bedrohungsanalyse bekannter Kampagnen ▪ Analyse von Bedrohungsgruppen oder -akteuren ▪ Zielgerichtete retrospektive Angriffsanalyse ▪ Vergleichsbericht zur Schutzeffizienz ▪ Retrospektive Angriffsanalyse von Benutzer-Kompromittierungsindikatoren	Beantwortet die Frage: Besteht für mich ein Risiko? Werde ich von einem konkreten Bedrohungsakteur angegriffen? Wird sich seine Kampagne wahrscheinlich gegen mich richten?
Wie gut ist meine Sicherheitsaufstellung insgesamt?	▪ Einheitliche Sicherheitsaufstellung vom Endgerät bis in die Cloud	Analyse und Optimierung aller meiner Sicherheitsprozesse
Bietet meine aktuelle Schutzkonfiguration ausreichenden Schutz?	▪ Überprüfung der lokalen Schutzlösungen	Analyse meiner aktuellen Sicherheitsaufstellung
Was muss ich für zuverlässigen Schutz konkret ändern?	▪ Überprüfung der lokalen Schutzlösungen	Empfehlungen zu notwendigen Maßnahmen
Können meine anderen Sicherheits-funktionen die Bedrohungen isolieren?	▪ Anweisung anderer Sicherheitsfunktionen zur Isolierung/Quarantäne	Senden von Aufforderungen zu Eindämmungsmaßnahmen an andere Sicherheitsfunktionen (per Data Exchange Layer, DXL), um das Risiko weiter verringern

Weitere Informationen

Weitere Informationen erhalten Sie unter www.mcafee.com.

McAfee

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