McAfee Investigator

Aus Analysten werden Untersuchungsexperten

McAfee® Investigator unterstützt Analysten bei der Ursachenanalyse und damit bei der schnelleren Behebung von Problemen. Auf Triage-Prüfungen beruhende Warnmeldungen lösen von Experten geführte Untersuchungen aus, bei denen unterstützende Daten erfasst, Hinweise interpretiert und die zur vollständigen sowie schnellen Validierung und Reaktion benötigten Informationen präsentiert werden.

Herausforderungen bei Sicherheitsabläufen

Die große Anzahl von Ereignissen sowie Probleme mit der Aufbewahrungsdauer von Daten erschweren die zuverlässige Analyse der in enormen Zahlen anfallenden Warnungen. Da den Analysten häufig der Kontext oder das Fachwissen für die Entscheidung fehlt, ob bestimmte Warnungen als Vorfall eingestuft werden sollten, werden sie oft schlichtweg ignoriert.

Die Untersuchung von Vorfällen kann daher lange dauern und erhebliches Fachwissen verschiedener Bedrohungsvektoren erfordern, um zum Kern des Problems zu gelangen. Durch diese Entwicklung wächst der Bedarf nach kompetenten Sicherheitsanalysten, während die Zahl entsprechender Spezialisten gleich bleibt.

Neue investigative Analysen

Zur Lösung dieses Problems müssen Sicherheitsteams die Triage-Prüfung von Warnmeldungen und die Untersuchung optimieren und beschleunigen, damit die vorhandenen Mitarbeiter und Junior-Analysten produktiver arbeiten können.

McAfee Investigator stellt allen Sicherheitsteams geführte Untersuchungen einschließlich Triage-Prüfungen, umfassender Datenerfassung und hochentwickelter Analysen zur Verfügung. Als SaaS-Angebot können Expertensysteme und Tools zur Endgeräteerfassung in vorhandene Datenquellen sowie Sicherheitsverwaltungssysteme integriert werden und so die Rendite beschleunigen und den Aufwand verringern.

Diese interaktiven Analysen bieten regelmäßig aktualisierte Hinweise, um Sicherheitsverantwortliche bei der vollständigen Untersuchung von Malware, Netzwerkbedrohungen und Kompromittierungsindikatoren in weniger Zeit und mit höherer Genauigkeit zu unterstützen.

Informationsgewinnung mit Maschinengeschwindigkeit

McAfee Investigator erlaubt die sofortige Verbesserung von Triage-Prüfungen, indem die Sicherheitsverantwortlichen bestimmte Situationen automatisch für sofortige Untersuchungen priorisieren können.

Wichtige Vorteile

- **Reduzierte Verweilzeit:** Ausführliche Untersuchung von Falldaten verbessert die Erkennung von Ursachen, anstatt lediglich Symptome zu beheben
- **Wechsel von Warnmeldungen zu Fällen:** Verringerter Zeitaufwand für manuelle Untersuchungen und Untersuchungen mit niedriger Priorität
- **Fokus auf das Unbekannte:** Aufspüren einmaliger Artefakte und Informationen, die menschliche Interpretation und Entscheidungen erfordern
- **Verbesserte Triage-Prüfungen:** Schnellere und präzisere Verarbeitung von mehr Fällen
- **Geringere Arbeitsbelastung für Analysten:** Bestmögliche Nutzung begrenzter Kapazitäten in Bezug auf Zeit, Energie und Kompetenzen
- **Aufbau von Analysekompetenzen:** Leitfäden und relevante Einblicke informieren Analysten über die richtigen Fragen und Hypothesen im Workflow

Für diese Alarme sowie weitere Warnungen, die Analysten untersuchen sollten, führt McAfee Investigator die Erfassung, Organisation, Zusammenfassung und Visualisierung der Warnungen, Aktivitäten, Nachweise und Einblicke zu einem vermuteten Angriff durch.

Relevante Daten werden im Hintergrund erfasst und umfassen lediglich Informationen, die für eine bestimmte Bedrohungsuntersuchung und zum Treffen einer Entscheidung notwendig sind. Daten aus SIEM-Lösungen (Sicherheitsinformations- und Ereignis-Management) können durch Daten von Endgeräten ergänzt werden, ohne dass auf jedem Node EDR-Agenten (Endpoint Detection and Response) ausgeführt werden müssen. Dieses Modell ersetzt isolierte Silos durch kontextbezogene Einblicke in Kompromittierungsindikatoren, Taktiken, Techniken, Verfahren und Beziehungen.

Ein Modul für Datenanalyse und Machine Learning vergleicht Nachweisdaten mit bekannten Basislinien sowie Bedrohungsdatenquellen, verarbeitet Artefakte und eskaliert wichtige verdächtige Erkenntnisse.

Durch die automatische Erfassung und Priorisierung der richtigen Daten verringert McAfee Investigator den Aufwand und erhöht die Geschwindigkeit, mit der Analysten das Risiko sowie die Dringlichkeit des Zwischenfalls ermitteln können. Analysten können zuverlässige Triage-Entscheidungen schneller treffen und sich auf die schwerwiegendsten Bedrohungen konzentrieren.

Auf Unternehmensebene sind die Vorteile noch größer. Durch die Erweiterung von Triage-Prüfungen von Warnungsüberprüfungen zu kontextabhängigen Fällen können die jeweiligen Analysten effizienter vorgehen, da mehr Fälle von Ebene-1-Analysten disponiert werden und die Zeit der Analysten bestmöglich genutzt wird.

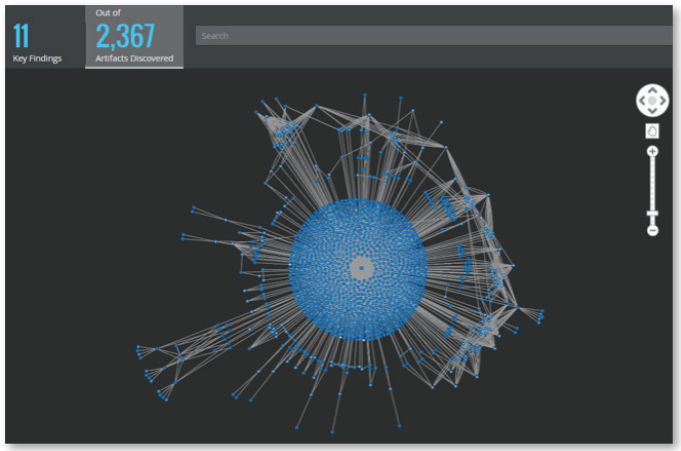

Abbildung 1. McAfee Investigator erfasst tausende Nachweise.

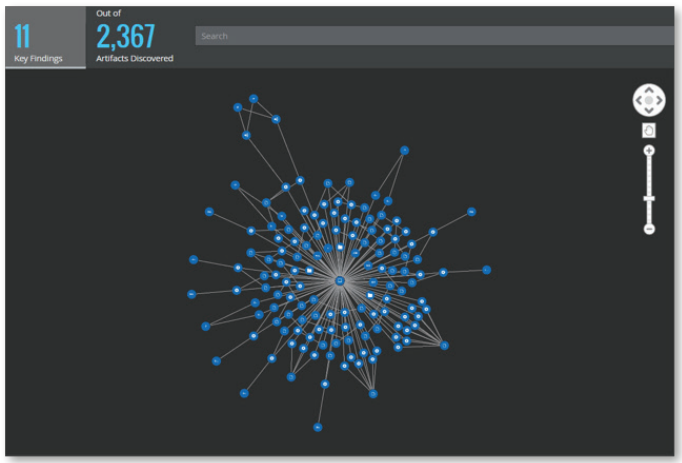

Abbildung 2. Anschließend nutzt McAfee Investigator Expertenanalysen und Hinweise, um beweiskräftige Fakten zu präsentieren.

Wichtige Vorteile (Fortsetzung)

- **Größerer Mehrwert vorhandener Systeme:** Vorhandene Datenquellen und Analysen werden erweitert, um Fokus und Genauigkeit zu verbessern

Kernfunktionen

- Präzise On-Demand-Datenerfassung
- Temporärer Agent zur Erfassung von Endgerätedaten
- Interpretation erfasster Daten basierend auf Expertenwissen und künstlicher Intelligenz
- Interaktive Virtualisierungen
- Vielseitige Hypothesen zur Untersuchung wahrscheinlicher Daten
- Basislinien für institutionelle Informationen
- Fall-Management mit Anweisungen für Mitarbeiter und Möglichkeit zum Informationsaustausch während der gesamten Untersuchung

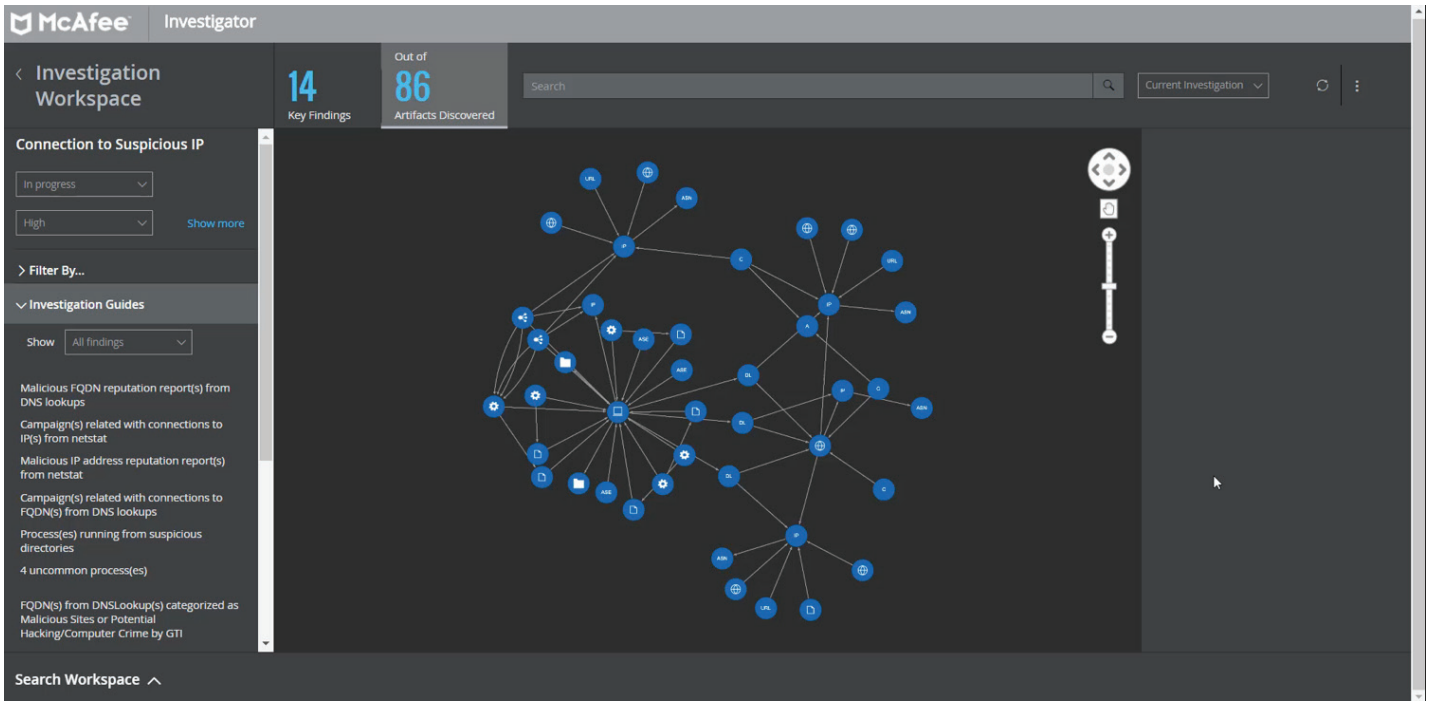

Abbildung 3. Der Arbeitsbereich stellt wichtige Erkenntnisse übersichtlich und leicht verständlich dar.

Geführte Untersuchungen mit Expertenwissen

Wenn ein Zwischenfall für eine genauere Untersuchung ausgewählt wird, können Analysten interaktive Leitfäden nutzen, die ihnen wichtige Hinweise für die Ermittlung des Umfangs sowie für Analysen geben. Die investigativen Leitfäden sind nicht skriptbasiert oder statisch. Das System imitiert menschliche Gedankengänge und überprüft gleichzeitig zahlreiche Theorien, um noch schneller und zuverlässiger zu einem Ergebnis zu kommen.

In die für Benutzer lesbaren Leitfäden flossen das Fachwissen der Foundstone®-Forscher sowie künstliche Intelligenz ein. Dies ist ein Aspekt, mit dem McAfee Investigator die Zusammenarbeit von Mensch und Maschine fördert.

Der Arbeitsbereich strukturiert Fallinformationen sowie Erkenntnisse und hilft auf diese Weise Analysten dabei, die richtigen Fragen zu stellen. Dieser konzentrierte, vielseitige Untersuchungsansatz ermöglicht die effiziente und zuverlässige Lösung von Fällen mit der großen Sicherheit, dass die Analysten die zugrunde liegende Ursache gefunden haben.

Skalierung von Fachwissen und Kapazität

Der interaktive Arbeitsbereich von McAfee Investigator ermöglicht Workflows und die Navigation durch Daten in einer einzigen intuitiven Umgebung. Dieses Modell steigert die Effizienz und verringert die Informationsüberflutung durch eine Vielzahl von Warnungstypen. Zudem sind für die Arbeit nicht mehr mehrere Bildschirme notwendig.

Im Arbeitsbereich können sich unerfahrene sowie fortgeschrittene Analysten mit den Gedankengängen erfahrener Analysten vertraut machen und sich auf diese Weise ohne zusätzliche Schulung Fähigkeiten aneignen.

Nutzung vorhandener Tools und Daten

McAfee Investigator arbeitet mit SIEM-Software und McAfee® ePolicy Orchestrator® zusammen, um vorhandene Datenquellen, Schwellenwerte, Korrelationen und Warnungen durch hochentwickelte Analysen zu ergänzen. Ein temporärer Agent erfasst neue Endgerätedaten, die für die zuverlässige Interpretation subtiler Hinweise besonders wichtig sind. Dank der Integration zwischen McAfee Investigator und McAfee Active Response können Analysten die Auswirkungen einer Bedrohung auf die Endgeräte in Echtzeit ermitteln. Über einen Aktivitäts-Feed werden Daten für Drittanbieter-Tools weitergegeben, damit sie in aktuelle Workflows integriert werden können, um Prozesse zu optimieren und die Zusammenarbeit zu verbessern. Professional Services erleichtern das Onboarding und die erfolgreiche Aktivierung.

Weitere Informationen

Mit McAfee Investigator müssen Sie bei einem Verdacht nicht mehr mehrere Stunden lang nach Daten suchen und anschließend noch mehr Zeit mit der Auswertung dieser Daten verbringen. Das hochentwickelte Analysemodul von McAfee Investigator untersucht Bedrohungswarnungen in einer kontextgesteuerten Benutzeroberfläche, um Sicherheitsabläufe zu skalieren. McAfee Investigator automatisiert die Nutzung von Expertenwissen in SOC-Untersuchungen, sodass Ihre Analysten schneller, gezielter und präziser arbeiten können.

Das ist der Vorteil der Zusammenarbeit von Mensch und Maschine.

Weitere Informationen erhalten Sie unter **www.mcafee.com/de/products/investigator.aspx**.

McAfee
Together is power.

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