Kurzvorstellung

Nutzung von Bedrohungsdaten

Hinter fast jeder echten Warnung, die bei Ihrem IT-Sicherheitsteam eingeht, steckt ein Gegner, der mit verschiedenen Angriffstechniken in Ihre Infrastruktur eindringen und Ihre wichtigen Daten oder Systeme kompromittieren möchte. Dabei umfassen die gezielten, mehrphasigen Angriffe von heute eine Reihe von Schritten, die zusammen eine Angriffskette aus Ausspähung, Schwachstellensuche, Ausnutzung und schließlich Exfiltration wertvoller Unternehmensdaten bilden.

Sicherheitsanalysten sind sich dieser Techniken absolut bewusst und benötigen Bedrohungsdaten, um Einblick in die Methoden und Motive der Angreifer zu erhalten. Anhand solcher Daten können sie hochentwickelte Bedrohungen erkennen und ausschalten sowie geeignete Behebungsmaßnahmen ergreifen. Zudem ermöglichen es diese Daten, sich besser auf die nächste Sicherheitswarnung vorzubereiten. Häufig fehlt jedoch entweder der Einblick in bestimmte Systeme, oder die IT-Mitarbeiter werden mit einer wahren Datenflut überschwemmt, die zu wenige nützliche Informationen enthält. Laut der Untersuchung des SANS Institute *Who's Using Cyberthreat Intelligence and How?* (Von wem und wie werden Informationen zu Internetbedrohungen genutzt?) „... können nur 11,9 Prozent der Befragten die Bedrohungsdaten aus praktisch jeder Quelle aggregieren und nur 8,8 Prozent sich ein vollständiges Bild verschaffen, in dem Ereignisse mit Kompromittierungsindikatoren verbunden werden."[1]

Einem aktuellen Forrester-Bericht zufolge sind 77 Prozent der Sicherheits-Entscheidungsträger in nordamerikanischen und europäischen Unternehmen der Meinung, dass die Verbesserung der Bedrohungsdaten Priorität hat.[2] Dank Informationen zu Cyber-Bedrohungen werden Sicherheitsexperten frühzeitig vor Cyber-Kriminellen gewarnt, die ihre Region, Branche oder bestimmte Unternehmen im Visier haben, und erhalten haben so Zeit, entsprechende Gegenmaßnahmen zu ergreifen. Nichtsdestotrotz steht der Bereich IT-Sicherheit noch vor großen Herausforderungen:

- Erfassung von Bedrohungsdaten aus externen sowie internen Quellen
- Datenkorrelation und Risikopriorisierung
- Datenverteilung an unternehmensweite Sicherheitskontrollen mehrerer Anbieter
- Größere Transparenz der IT-Landschaft für angemessene und schnelle Gegenmaßnahmen

intel Security

Moderne Unternehmen benötigen eine offene, integrierte Architektur, mit der die Implementierung von Bedrohungsdaten vereinfacht und deren Vorteile genutzt werden können. Diese Vorteile reichen von der grundlegenden Erfassung von Bedrohungsdaten für forensische Analysen bis hin zur Nutzung dieser Daten zur Ergänzung von SIEM-Analysen. Mit anderen Worten: Benutzer müssen Bedrohungsdaten über automatisierte Prozesse einsetzen, die sie bei der Analyse, Verarbeitung sowie Verwaltung dieser Daten unterstützen.

Neue Bedrohungen verlangen einen neuen Ansatz für Bedrohungsdaten

In Anbetracht der immer komplexeren, genaueren und umfangreicheren Angriffe reicht der bisher bewährte Ansatz für Bedrohungsdaten nicht mehr aus. Die Untersuchung gezielter Angriffe ist jedoch keine leichte Aufgabe. Aufgrund des dynamischen Verhaltens der Angreifer, der größeren Vielseitigkeit sowie Verfügbarkeit lokaler und globaler Bedrohungsdatenquellen sowie der Vielfalt der Bedrohungsdatenformate kann die Einbindung und Verarbeitung von Bedrohungsdaten in den Tools des Sicherheitskontrollzentrums zu einer größeren Herausforderung werden als jemals zuvor.

Eine aus verschiedenen Anbietern bestehende Umgebung, wie sie für die meisten Unternehmen typisch ist, erschwert den Austausch von Ereignisdaten und die Förderung der Ereignistransparenz im Unternehmen zusätzlich. Wie das Marktforschungsunternehmen Gartner in seinem Bericht *Technology Overview for Threat Intelligence Platforms* (Technologieüberblick über Bedrohungsdaten-Plattformen) aufzeigt, „profitieren Cyber-Kriminelle vom fehlenden Austausch der Bedrohungsdaten in Unternehmen. Der Bedrohungsdatenaustausch ist ein starkes und zunehmend wichtiges Element, um mit der immer größeren Zahl an Bedrohungsakteuren sowie den von ihnen genutzten Angriffen Schritt zu halten.“[3]

Der Austausch von Bedrohungsdaten allein führt jedoch nicht zwangsläufig zu nachhaltigen Korrektur- und Schutzmaßnahmen. Sicherheitsanalysten können von zu vielen Informationen schnell überfordert sein. Immerhin müssen die meisten Sicherheitsteams noch aufwändige manuelle Prozesse befolgen (siehe Abbildung 1). Dabei analysieren sie Millionen Sicherheitsereignisse und verdächtige Dateien, um Datenberge wie Puzzleteile zusammenzusetzen und den gezielten Angriff zu rekonstruieren. Letztlich wirkt sich diese Vorgehensweise negativ auf die Gründlichkeit und die Geschwindigkeit des Reaktionsprozesses aus. Wenn Sicherheitsteams Bedrohungen nicht bis ins Detail verstehen, wird es ihnen immer schwer fallen, Angriffe zeitnah einzudämmen. In einer 2014 veröffentlichten Studie von Intel Security *When Minutes Count* (Wenn es um Minuten geht) sahen sich weniger als 25 Prozent der Befragten in der Lage, einen Angriff innerhalb weniger Minuten zu erkennen.[4]

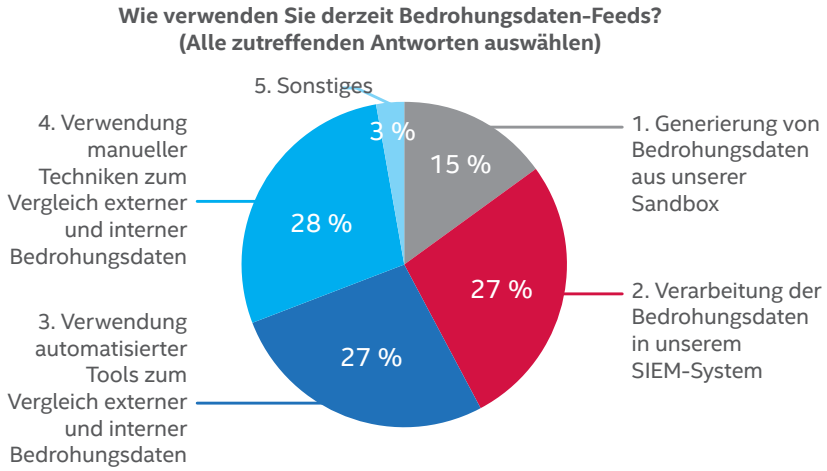

Abbildung 1. Eine während der BlackHat-Konferenz 2015 durchgeführte Umfrage von Intel Security ergab, dass viele Benutzer externe Bedrohungsdatenquellen und interne Bedrohungsdaten noch immer anhand manueller Techniken vergleichen.

„Für unsere Sicherheitsinfrastruktur haben wir viel mehr gebraucht, als ein Technologie-Anbieter liefern kann. Wir mussten deshalb unbedingt eine Beziehung zu einem Partner aufbauen, der uns bei der Verwaltung unserer vielfältigen Kundenanforderungen und der sich ständig wandelnden Bedrohungen unterstützen kann. Mit McAfee haben wir einen solchen Partner gefunden. Und dank der laufenden Sicherheitsdaten, die wir über McAfee-Lösungen erhalten, können wir unseren Geschäftsbetrieb stets auf dem neuesten Stand halten.“

– Anurana Saluja
CISO und Vice President
of Information Security
Sutherland Global Services

Nutzung von Bedrohungsdaten

Für die informationsgesteuerte Erkennung von und Reaktion auf Bedrohungen reicht es nicht aus, die schädlichen IP-Adressen, die auf einer offenen Webseite veröffentlicht werden, einmal pro Woche manuell in eine SIEM-Watchlist zu importieren. Vielmehr müssen Bedrohungsdaten in Echtzeit aufgenommen und alle Facetten eines Angriffs, einschließlich Methoden und weltweiten Kampagnen, korreliert werden, damit Unternehmen auch den heimlichsten und wandelbarsten Bedrohungen zuvorkommen können. Darüber hinaus müssen die Sicherheitskontrollzentren der Unternehmen eine Möglichkeit finden, wie sie Bedrohungsdaten nutzen können, um ein vollständiges Bild der Angriffe auf ihre Umgebungen zu erhalten. Zur Analyse, Korrelation und Priorisierung der Bedrohungsdaten müssen sie enorme Datenmengen durchsuchen und herausfinden, welche Informationen für ihre Branche, ihre Region sowie ihr Unternehmen relevant sind. Zudem müssen sie sich einen Überblick über einmalige Angriffe der Gegenwart sowie Trends verschaffen können. Dazu werden Daten zu vergangenen Sicherheitsereignissen herangezogen. Auch Forrester stuft die Nutzung von Bedrohungsdaten als wichtig ein, da sich 75 Prozent der Angriffe innerhalb von 24 Stunden von einem Opfer zum nächsten ausbreiten. Die Unternehmen müssen also die Lücke zwischen „Austauschgeschwindigkeit und Angriffsgeschwindigkeit“ schließen.[5]

Nutzung der integrierten Intel Security-Architektur

Intel Security liefert eine einheitliche, kollaborative Plattform mit allen Komponenten für die Nutzung von Bedrohungsdaten. Dazu zählen Feeds zu weltweiten Bedrohungsinformationen, lokal erfasste Daten, der Echtzeitaustausch von Bedrohungsdaten in der IT-Infrastruktur, das Sicherheitsinformations- und Ereignis-Management sowie die Bereitstellung automatischer, adaptiver Schutzmaßnahmen.

Voraussetzungen für die Bedrohungs-analyse	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
Erfassung von Bedrohungsdaten aus externen Quellen	STIX, McAfee Global Threat Intelligence (McAfee GTI)-Import sowie VirusTotal	McAfee GTI-Import	McAfee GTI- und TAXII/STIX-Import sowie HTTP-Bedrohungsdaten-Feeds über die Lösung McAfee Enterprise Security Manager zur Verwaltung von Cyber-Bedrohungen	McAfee GTI aggregiert Bedrohungsdaten von zahlreichen Cyber Threat Alliance-Partnern und öffentlichen Quellen. McAfee GTI erfasst Bedrohungsdaten von Millionen Sensoren auf Intel Security-Produkten, die bei Kunden auf Endgeräten, Web-, E-Mail- und Netzwerk-eindringungsschutz-Systemen sowie Firewall-Geräten im Einsatz sind.
Erfassung interner Bedrohungsdaten	Erfasst Daten von McAfee VirusScan®, McAfee Application Control, McAfee Web Gateway, McAfee Advanced Threat Defense, McAfee Enterprise Security Manager sowie von Drittanbieter-Produkten, die Informationen über den McAfee Data Exchange Layer senden	Verarbeitet Beispieldateien, die über McAfee Threat Intelligence Exchange oder das Netzwerk eingehen, um die Bedrohung zu neutralisieren	Über STIX/TAXII und den McAfee Data Exchange Layer	

Schaffung lokaler Bedrohungsdaten	Erfasst Vorfälle mit verdächtigen Dateien und erstellt eine lokale Datenbank zur Aufzeichnung des Erstkontakts sowie zur der Bewegung der Bedrohungen	Analysiert und überführt Malware, generiert lokale Bedrohungsdaten und verbreitet diese über den McAfee Data Exchange Layer oder als API im STIX-Format	Erstellt anhand korrelierter Ereignisse Watchlists, Berichte und Ansichten zu Bedrohungsdaten	
Verbreitung von Bedrohungsdaten über Sicherheits-kontrollen	Über den McAfee Data Exchange Layer	Über den McAfee Data Exchange Layer und die Produkt-API	Über den McAfee Data Exchange Layer, die Produkt-API und Skript-Integration	McAfee GTI ist in zahlreiche Intel Security-Produkte integriert, z. B. McAfee Web Gateway, McAfee Enterprise Security Manager und McAfee-Endgerätelösungen
Überblick über die erfassten Bedrohungsdaten	Über McAfee Threat Intelligence Exchange-Dashboards	Über Berichte	Über Dashboards, Ansichten, Berichte aus Inhaltspaketen und kundenseitig generierte Berichte	Über das McAfee Threat Center und den vierteljährlichen Threat-Report von McAfee

Tabelle 1. Die integrierte Bedrohungsdaten-Plattform von Intel Security

Erfassung, Analyse und Verbreitung

McAfee Global Threat Intelligence

Am besten beginnen Sie den Aufbau Ihrer integrierten Bedrohungsdaten-Plattform mit McAfee Global Threat Intelligence (McAfee GTI), einem umfassenden, in Echtzeit arbeitenden und Cloud-basierten Reputationsdienst. Er ist vollständig in Intel Security-Produkte integriert und unterstützt die Produkte dabei, Cyber-Bedrohungen aus allen Vektoren – Dateien, Internet, E-Mails und Netzwerk – schnell und besser abzuwehren. McAfee GTI liefert Reputationsbewertungen für Millionen Dateien, URLs, Domänen und IP-Adressen. Die dafür verwendeten Bedrohungsdaten stammen aus zahlreichen Quellen, z. B. von Millionen globalen und von McAfee Labs überwachten sowie analysierten Sensoren, aus Bedrohungsdaten von Forschungs- und Cyber Threat Alliance-Partnern sowie von Bedrohungsinformationen zu den Vektoren Internet, E-Mails und Netzwerke. Auf Grundlage dieser hochwertigen, relevanten Bedrohungsdaten gibt McAfee GTI genaue Hinweise zu Risiken und unterstützt damit nicht nur informierte Richtlinienentscheidungen, sondern ermöglicht auch Kontrollen, mit denen Elemente bei Bedarf blockiert, bereinigt oder zugelassen werden können.

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (SIEM) bietet eine Schnittstelle für die Konsolidierung, Analyse sowie Reaktion auf jede Art von Bedrohungsdaten und hebt damit die Erfassung sowie Analyse von Bedrohungsdaten auf die nächste Stufe. Diese Rundumsicht gewährt volle Transparenz und Situationserkennung, wodurch gezielte Angriffe schneller erkannt und bekämpft werden können. Zudem wurde das Datenverwaltungssystem dieser Komponente speziell für die Echtzeit-Speicherung und -Integration großer Mengen an Kontextdaten entwickelt.

Was ist die Cyber Threat Alliance?

Die **Cyber Threat Alliance** ist eine Gruppe von Sicherheitsexperten aus unterschiedlichen Unternehmen, deren Ziel es ist, Bedrohungsdaten auszutauschen und die Abwehr von Bedrohungen in Mitgliedsunternehmen und bei deren Kunden zu verbessern. Intel Security ist eines der Gründungsmitglieder, die alle ihre Ressourcen dafür einsetzen, den effektivsten Weg zum Austausch von Bedrohungsdaten zu bestimmen, die Zusammenarbeit der Mitglieder zu fördern und gemeinsam Fortschritte im Kampf gegen raffinierte Cyber-Kriminelle zu erzielen.

McAfee Enterprise Security Manager erfasst Aktivitäts- und Ereignisdaten aus allen Ihren Systemen, Datenbanken, Netzwerken sowie Anwendungen. Zusätzlich importiert die Lösung globale Bedrohungsdaten und verarbeitet Bedrohungsinformationen aus Standardformaten und -übertragungen wie Structured Threat Information eXpression (STIX) bzw. Trusted Automated eXchange of Indicator Information (TAXII) und CybOX, die in der Regel von Community- oder Branchengruppen wie dem Financial Services Information Sharing and Analysis Center (FS-ISAC) veröffentlicht werden. Mittels hochentwickelter Analysen werden die gesammelten Informationen in verständliche, umsetzbare Sicherheitsdaten umgewandelt. Wesentlich bedeutender sind jedoch der detaillierte Einblick in neue Bedrohungen über Echtzeit-Ansichten sowie der Zugang zu älteren Sicherheitsdaten. Durch die Untersuchung vergangener Ereignisse können Sie die Ausbreitung sowie Muster eines Angriffs verstehen und automatisierte Watchlists erstellen, um in Zukunft neue oder wiederholt auftretende Ereignisse zu erkennen. Durch die stärke Sensibilisierung Ihres Systems für bekanntermaßen böswillige Ereignisse verbessern Sie nicht nur die Erkennung verdächtiger Aktivitäten und der Muster solcher Aktivitäten in den verschiedenen Phasen der Angriffskette, sondern können auf dieser Grundlage auch Ihre Reaktionen priorisieren.

Abbildung 2. Ansicht von McAfee GTI.

McAfee GTI for McAfee Enterprise Security Manager nutzt die Leistungsfähigkeit der McAfee Labs-Forschungsmöglichkeiten für die Überwachung der Unternehmenssicherheit. Dieser ständig aktualisierte, umfangreiche McAfee GTI-Feed verbessert die Situationserkennung durch die schnelle Erkennung von Ereignissen, bei denen mit verdächtigen oder böswilligen IP-Adressen kommuniziert wird. Darüber hinaus können Sicherheitsadministratoren bestimmen, welche Unternehmens-Hosts derzeit mit als böswillig bekannten Akteuren kommunizieren oder kommuniziert haben.

McAfee Threat Intelligence Exchange
Als dritte Komponente bei der Entwicklung eines integrierten Ökosystems für Bedrohungsdaten können Sie mit McAfee Threat Intelligence Exchange eine Lösung hinzufügen, die Dateireputationsdaten in der gesamten Sicherheitsinfrastruktur aggregiert und austauscht. McAfee Threat Intelligence Exchange empfängt neben Bedrohungsdaten aus McAfee GTI, STIX-Dateiimporten und über McAfee Enterprise Security Manager erfassten Bedrohungs-Feeds auch Informationen, die von Endgeräten, Anwendungskontrollen, Mobilgeräten, Gateways, Rechenzentren und Sandbox-Technologien in Intel Security- und Drittanbieter-Lösungen stammen. Durch die Datenerfassung in allen Bereichen Ihrer Infrastruktur erhalten Sie Informationen zu Bedrohungen, die möglicherweise nur in Ihrer Umgebung auftreten – wie es für viele gezielte Angriffe üblich ist. Die Dateireputationsdaten wiederum werden über den McAfee Data Exchange Layer sofort an alle mit McAfee Threat Intelligence Exchange verknüpften Produkte und Lösungen im gesamten Ökosystem weitergegeben. Wenn McAfee Threat Intelligence Exchange beispielsweise Informationen über eine böswillige ausführbare Datei verbreitet, erhält McAfee Data Loss Prevention diese Information über den McAfee Data Exchange Layer und überwacht diese ausführbare Datei dann auf sensible Dateizugriffe.

Zu den über den McAfee Data Exchange Layer ausgetauschten Bedrohungsdaten gehören Dateireputationen, Datenklassifizierungen, Anwendungsintegrität sowie Kontextinformationen zu Benutzern, wobei diese Daten mit und zwischen Produkten ausgetauscht werden, die in die McAfee Data Exchange Layer-Struktur integriert sind. Alle Produkte und Lösungen können in den McAfee Data Exchange Layer integriert werden. Anschließend legen Sie fest, welche Informationen an das System gesendet bzw. überwacht und abonniert werden sollen.

McAfee Threat Intelligence Exchange arbeitet eng mit McAfee Advanced Threat Defense, der modernen Sandbox-Lösung von Intel Security, zusammen, die McAfee Threat Intelligence Exchange mit Malware-Analysedaten versorgt. Wenn eine Datei als böswillig erkannt wird, sendet McAfee Threat Intelligence über den McAfee Data Exchange Layer ein Dateireputations-Update an alle verbundenen Systeme. Dieser Prozess funktioniert aber auch umgekehrt. Wenn Endgeräte mit McAfee Threat Intelligence Exchange Dateien mit unbekannter Reputation erkennen, werden diese an McAfee Advanced Threat Defense weitergeleitet. Die Lösung überprüft dann, ob das Objekt böswillig ist, und schließt dadurch Erkennungslücken durch die Out-of-Band-Übertragung von Schaddaten. Gemeinsam liefern diese beiden Produkte automatisierten, adaptiven Schutz vor neuen Bedrohungen. Informationen über erkannte Angriffe werden in der gesamten Umgebung verteilt, damit die Angriffskette unterbrochen wird, ehe weiterer Schaden entsteht.

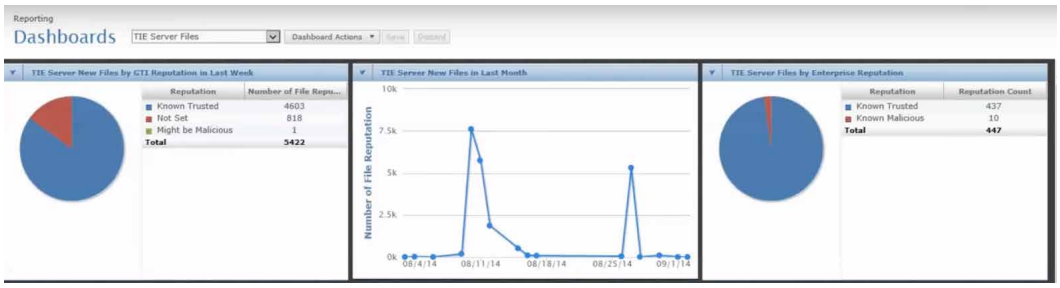

Abbildung 3. McAfee Threat Intelligence Exchange-Dashboard.

McAfee Threat Intelligence Exchange ermöglicht dank übergreifender Datennutzung in Sicherheitslösungen für Endgeräte, Gateways, Netzwerke sowie Rechenzentren adaptive Bedrohungserkennung und -abwehr in Echtzeit. Durch die Kombination und die sofortigen Weitergabe globaler Bedrohungsinformationen sowie lokal erfasster Daten können Ihre Sicherheitslösungen als Einheit fungieren, die nicht nur Informationen austauscht, sondern auch auf Basis gemeinsamer Informationen agiert.

Unterbrechung der Angriffskette

Unabhängig davon, wo der Erstkontakt durch eine unbekannte Malware-Datei stattfand, wird die gesamte verbundene Umgebung unmittelbar nach der Erkennung aktualisiert. Wenn eine Datei von McAfee Advanced Threat Defense überführt wurde, veröffentlicht McAfee Threat Intelligence Exchange diese Bedrohungsinformationen in einem Reputations-Update über den McAfee Data Exchange Layer an alle Sicherheitskontrollen im Unternehmen. Gateways mit McAfee Threat Intelligence Exchange verhindern, dass die Datei in Ihre Infrastruktur gelangt. Durch den koordinierten Austausch von Bedrohungsdaten zwischen allen Sicherheitskontrollen kann die Angriffskette ohne manuelle Eingriffe problemlos unterbrochen und damit weiterer Schaden verhindert werden.

Verarbeitung und Anwendung für genauere Erkennung und bessere Entscheidungen

Nachdem Bedrohungsdaten erfasst wurden, fungiert McAfee Enterprise Security Manager als zentraler Punkt, der einen Gesamtüberblick gewährt und an dem die McAfee GTI- und McAfee Threat Intelligence Exchange-Feeds sowie die im STIX/TAXII-Format vorliegenden Kompromittierungsindikatoren mit Ereignisdaten korreliert werden, die in Echtzeit oder aus Verlaufsdaten ermittelt wurden, wenn Nodes in Ihrem Netzwerk mit böswillig bekannten Akteuren oder verdächtigen Domänen kommunizieren. Im Bedrohungsverwaltungs-Dashboard erhalten Analysten eine zentrale Gesamtansicht aller erfassten Bedrohungsindikatoren, der Datenquellen, der Trefferquoten gegenüber den Indikatoren sowie der wichtigsten Details zu Kompromittierungsindikatoren.

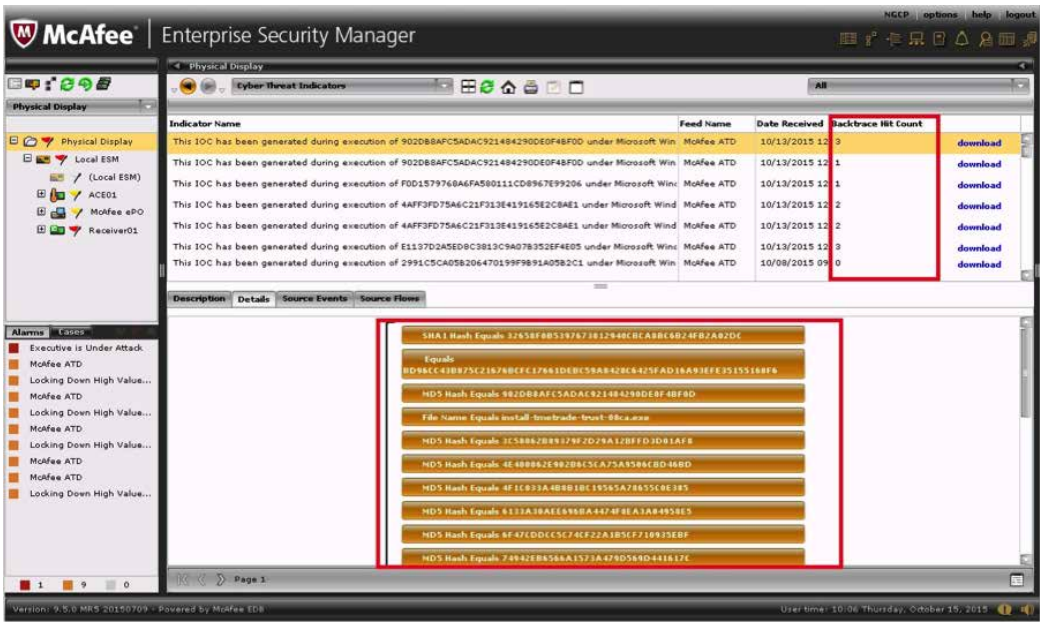

Abbildung 4. In McAfee Enterprise Security Manager angezeigte Indikatoren für Cyber-Bedrohungen, Treffer basierend auf Verlaufsdaten und Details zu Kompromittierungsindikatoren.

Durch die gemeinsame Nutzung des Intel Security-SIEM-Systems mit anderen gemeinschaftlich agierenden Tools für Bedrohungsdaten werden die Betriebsausgaben für die Konfiguration von Korrelationsregeln gesenkt, die meist in einem umständlichen manuellen Prozess erstellt werden müssen. Beispielsweise können Sicherheitsanalysten neue Bedrohungsdaten direkt in einem verständlichen Format ansehen und neu erkannte Bedrohungen besser verstehen. Noch bedeutender ist aber, dass empfangene Bedrohungsdaten automatisch in Korrelationsregeln zu Echtzeit- oder Verlaufsdaten übernommen werden können, was die Erkennung bereits laufender oder neuer schädlicher Aktivitäten beschleunigt. Zudem können Sie den Verlauf der gemeldeten Bedrohungen in Ihrer IT-Umgebung sowie über Kontextinformationen in Warnanzeigen verfolgen und dadurch nicht nur bessere, sondern auch informiertere Entscheidungen treffen. Alle erfassten Daten verbessern und beschleunigen die Erkennung sowie Untersuchung gezielter Angriffe.

Da sich Bedrohungen schnell ihren Weg durch die IT-Infrastruktur bahnen und ihre Gestalt im Laufe der Zeit immer wieder ändern, aktualisiert auch McAfee Enterprise Security Manager regelmäßig alle erfassten Bedrohungsdaten und löscht alte, weniger relevante Informationen. So werden beispielsweise entfernte Befehls- und Steuerungsserver oder bereinigte Webseiten, die als wenig schädlich eingestuft werden, automatisch gelöscht. Als Folge dessen wird Ihr Sicherheitsteam nicht durch False-Positive-Meldungen abgelenkt und kann sich um die echten Bedrohungen kümmern.

Die folgenden Intel Security-Produkte unterstützen Bedrohungsdaten im STIX-Format:

- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Detection
- McAfee Enterprise Security Manager

Zusammenfassung

Die in Intel Security-Lösungen integrierten Bedrohungsdatenfunktionen ermöglichen die Erfassung, Verarbeitung und Verwaltung von Bedrohungsdaten. Dadurch können Sie die Bedrohungserkennung verbessern, manuelle Eingriffe vermeiden und verhindern, dass Gegenspieler Ihr Unternehmen schädigen. Dank größerer Transparenz und Einblicke in böswillige Aktivitäten in Ihrem Sicherheitsökosystem können Sie gezielte Angriffe bereits heute besser erkennen bzw. ihnen zuvorkommen und sie zukünftig verhindern.

Weitere Informationen

Weitere Informationen zu den Bausteinen der integrierten Bedrohungsdaten-Plattform von Intel Security finden Sie unter:

- **McAfee Global Threat Intelligence**
- **McAfee Threat Intelligence Exchange**
- **McAfee Advanced Threat Defense**
- **McAfee Enterprise Security Manager**
- **How to Use a TAXII Feed with McAfee Enterprise Security Manager (Nutzung eines TAXII-Feeds mit McAfee Enterprise Security Manager)**

1. **https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767**
2. **https://www.forrester.com/The+State+Of+The+Cyberthreat+Intelligence+Market/fulltext/-/E-RES123011**
3. **https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms**
4. **http://www.mcafee.com/de/resources/reports/rp-when-minutes-count.pdf**
5. **https://www.rsaconference.com/writable/presentations/file_upload/cxo-t08r-threat-intelligence-is-like-three-day-potty-training.pdf**

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com