CYREN

Wirkungsvoller Einsatz von Bedrohungsinformationen zur Verbesserung der MTTR (Mean Time to Repair) und zur Unterstützung des Entscheidungsprozesses im SOC

Lösungsprofil

Eine geschäftliche Herausforderung

Mehr als 90% der Sicherheitsverletzungen bei Unternehmen beginnen mit einer einzigen E- Mail. Sicherheitsoperationsteams (SOCs) befinden sich zum Schutz ihres Unternehmens in einem ständigen Kampf gegen sich weiterentwickelnde feindliche Taktiken auf E-Mail-Basis. Das SOC stützt sich zur Entscheidungsfindung auf Daten – diese umfassen üblicherweise mehrere Bedrohungsinformationen-Feeds (kostenlos und entgeltlich) sowie interne Informationen. Bedrohungsinformationen dienen dazu, umsetzbare Einblicke zu gewähren, welche die Bedrohungsidentifizierung und Reaktionseffizienz verbessern. Dies wird durch eine Priorisierung der Bedrohungen erreicht, die unverzügliche Aufmerksamkeit erfordern. Aber nicht alle Bedrohungsinformationen-Feeds sind gleichwertig. Kostenlose Bedrohungsfeeds beziehen ihre "Daten" oft aus der gleichen Quelle und sind möglicherweise nicht immer fristgerecht oder von hoher Qualität. Unsachgemäß operationalisierte Informationen von geringer Qualität liefern nur einen begrenzten Wert und können oft das Arbeitspensum eines Sicherheitsanalysten erhöhen, was zu überforderten Sicherheitsteams und gesteigerter Verletzlichkeit der Organisation führt.

Vorteile der Lösung

- Gesteigertes Bewusstsein für neue und sich entwickelnde Bedrohungen auf E-Mail-Basis
- Umsetzbare, kontextbezogene Informationen zum Fällen zeitgerechter, aussagekräftiger Entscheidungen
- Verbesserte Wirksamkeit der Bedrohungsreaktion

Lösung von Herausforderungen durch Bedrohungsinformationen

Mangelnde Sichtweite - Teure Sicherheitsinvestitionen sind beim Stoppen der Übertragung bekannter, bestehender Bedrohungen per E-Mail wirksam. Aber was ist mit neuen und sich entwickelnden Bedrohungen? Der effektive Schutz des Unternehmens vor einer sich rapide entwickelnden Bedrohungslandschaft ist eine Herausforderung, der sich heutzutage viele Unternehmen gegenübersehen. Organisationen fehlt der Kontext, um die Auswirkungen sich entwickelnder Bedrohungen zu verstehen, und die erforderliche Sichtbarkeit zu ihrer Identifizierung, und sind dadurch verwundbar.

Mangel an zeitgerechter Information - Angesichts der ständigen Weiterentwicklung der Taktiken, Techniken und Verfahren der Angreifer ist die Zeit bei der Reaktion auf und der Eindämmung von Bedrohungen von entscheidender Bedeutung. Wenn sie nicht rechtzeitig operationalisiert werden, können Bedrohungsinformationen schnell veraltet sein und Ihre Organisation damit anfällig für sich schnell ändernde Angriffe durch opportunistische Angreifer werden.

Die Treffsicherheit im Erkennen und der Reaktion auf Bedrohungen verbessern - Anbieter von Bedrohungsdaten kaufen oft Informationen aus ähnlichen Quellen, die sie dann bündeln und als Informationsfeeds verkaufen. Da die SOCs von Unternehmen oft mehrere Bedrohungsdatenfeeds (kostenlos und entgeltlich) abonniert haben, stoßen sie bei der Treffsicherheit ihrer Bedrohungserkennung wegen ihrer gemischten Qualität auf Herausforderungen. Wertvolle Informationen können oft in Bergen alter Informationen oder falsch positiver Ergebnisse vergraben sein. Dies kann dazu führen, dass Gelegenheiten zum Erkennen von Bedrohungen verpasst werden und somit die Wirksamkeit ihrer Sicherheitsinvestitionen verringert wird.

25	1.3	300
Milliarden Sicherheitsabfragen pro Tag	Milliarden geschützte Benutzer	Millionen abgewehrte Gefahren pro Tag

Wirkungsvoller Einsatz von Bedrohungsinformationen zur Verbesserung der MTTR (Mean Time to Repair) und zur Unterstützung des Entscheidungsprozesses im SOC

Lösungsprofil

Cyren Threat InDepth

Bei Cyren Threath InDepth handelt es sich um kontextbezogene, korrelierte Bedrohungsdaten. Diese ermöglichen es Sicherheitsteams und deren Führungskräften, einen umfassenden und multidimensionalen Überblick über sich entwickelnde Bedrohungen auf E-Mail-Basis zu erlangen und sinnvolle Entscheidungen zu ihrer Bekämpfung zu treffen. Diese präzisen, umsetzbaren Informationen werden durch die Analyse und Bearbeitung von täglich Milliarden Transaktionen aus E-Mail-Inhalten, verdächtigen Dateien und Internetdatenaufkommen gewonnen, um schneller als andere Anbieter einzigartige, zeitgerechte Erkenntnisse liefern zu können. Threat InDepth ist für Unternehmen erhältlich als – **Phishing & Fraud URL Intelligence, Malware URL Intelligence, Malware File Intelligence und IP Reputation Intelligence.**

Vorteile von Threat InDepth

1. **Einzigartige Sichtweite zum Schutz vor bekannten & sich entwickelnden Bedrohungen:** Die Cyren GlobalView™ Threat Intelligence Cloud verarbeitet täglich Milliarden von Transaktionen, um Sicherheitsbedrohungen in E-Mails, Dateien und dem Internet zu identifizieren und Cyren damit die frühstmögliche Indikation neuer, sich entwickelnder Bedrohungen auf E-Mail-Basis zu liefern. Die urheberrechtlich geschützten Threat Engines von Cyren analysieren und gleichen diese Informationen ab und liefern damit Sicherheitsteams einen wertvollen Zusammenhang (erhältlich als Threat InDepth Intelligence), mit dem sie ein schnelleres Erkennen und eine schnellere Reaktion bewirken können. Durch die Kombination von menschlicher Intelligenz und fortschrittlichen Algorithmen ermöglicht Threat InDepth es Analysten, sich vor aller Augen verbergende neue und sich entwickelnde Bedrohungen zu erkennen und somit ihre frühe Identifizierung und Korrektur sicherzustellen.
2. **Beschleunigung der Bedrohungserkennung & Vorfallreaktion:** Analysten führen einen fortlaufenden Kampf zum Schutz ihres Unternehmens gegen sich entwickelnde Taktiken, Techniken und Verfahren von Angreifern. Zeitgerechte, kontextbezogene Bedrohungsdaten bemächtigen Sicherheitsteams dazu, kluge und sinnvolle Entscheidungen zu treffen. Durch die tägliche Analyse von Milliarden von E-Mails sind die Cyren Threat Engines in der Lage, IOCs schneller als andere Sicherheitsanbieter eindeutig zu identifizieren und zuzuordnen. Threat InDepth setzt diese Informationen wirkungsvoll ein und liefert Sicherheitsteams zeitgerechte, umsetzbare Erkenntnisse, Diese werden gebraucht, um Bedrohungen schnell zu identifizieren und zu priorisieren, darauf zu reagieren sowie die mittlere Zeit bis zur Entdeckung (Mean Time to Detect, MTTD) und mittlere Reaktionszeit (Mean Time to Respond, MTTR) zu reduzieren.
3. **Verbesserung des Werts von Sicherheitsmessungen:** Durch rechtzeitige Operationalisierung von Daten in ihren Sicherheitsinvestitionen können Unternehmen eine umfassende Sicherheitsaufstellung gewährleisten und aufrecht erhalten. Threat InDepth beliefert Sicherheitsteams schneller als andere Anbieter mit korrelierten, kontextbezogenen und zeitgerechten Daten. Durch die Aufnahme dieser präzisen Einblicke können Sicherheitstools die Effektivität ihrer Entdeckungen verbessern und den Teams einen multidimensionalen Überblick über die Bedrohungslandschaft bieten. Dies erlaubt es Organisationen, eine umfassende und proaktive defensive Aufstellung sicherzustellen und aufrecht zu erhalten.

IP Reputation Intelligence

Phishing & Fraud URL Intelligence

Malware URL Intelligence

Malware File Intelligence