PRODUKTÜBERSICHT

Endpoint Threat Analytics-Suite

LogRhythm
The Security Intelligence Company

Endpunkte sind seit langem beliebte Ziele von Cyber-Kriminellen, denn sie bieten zahlreiche Möglichkeiten für eine Kompromittierung. Angreifer setzen eine Reihe von Methoden ein, um Desktops, Laptops, Server und mobile Geräte zu infizieren. Um in ein Unternehmen einzudringen und zu kompromittieren nutzen sie beispielsweise Watering-Hole-Attacken, Phishing-oder Spear-Phishing-Angriffe sowie mit Schadsoftware manipulierte Websites. Doch obwohl ein offensichtlicher Bedarf an Verhaltensanalysen für Endpunkte besteht – insbesondere aufgrund der hohen Zahl an mobilen Mitarbeitern und der intensiven Nutzung privater mobiler Endgeräte (BYOD), vertrauen viele Unternehmen noch immer auf herkömmliche signaturbasierende Lösungen für den Schutz der Endpunkte vor Bedrohungen. Da die Malware und die Zero-Day-Attacken immer ausgefeilter werden und sich kontinuierlich verändern ist eine anspruchsvolle Lösung für die Überwachung der Endpunkte ein unverzichtbarer Bestandteil eines ganzheitlichen Security Intelligence-Ansatzes.

Analyse der Endpunkte

- ☑ Erkennung von Malware
- ☑ Konfigurationsanalyse und -überwachung
- ☑ Schutz vor Host-KOmpromittierungen
- ☑ Anwendung bewährter Sicherheitsverfahren

Die Endpoint Threat Analytics Suite von LogRhythm unterstützt Unternehmen dabei, die Bedrohungen für Endpunkte zu identifizieren und darauf zu reagieren sowie zu erkennen, ob kompromittierte Geräte von Angreifern für ihre böswilligen Aktivitäten genutzt werden. Die Endpoint Threat Analytics Suite umfasst ein Regelset für fortschrittliche VerhaltensAnalysen und sofortige Warnmeldungen, die ein ganzheitliches Bild der Bedrohung am Endpunkt en abgeben. So können Sicherheitsverantwortliche Geräte, die angegriffen werden oder schon kompromittiert sind, sehr einfach und schnell .auffinden n Zudem erhalten sie alle relevanten Kontext-Informationen zum jeweiligen Ereignis. Die Zeitspanne für die Eindämmung einer Bedrohung lässt sich damit erheblich reduzieren und sie können einen möglichen Schaden abwenden.

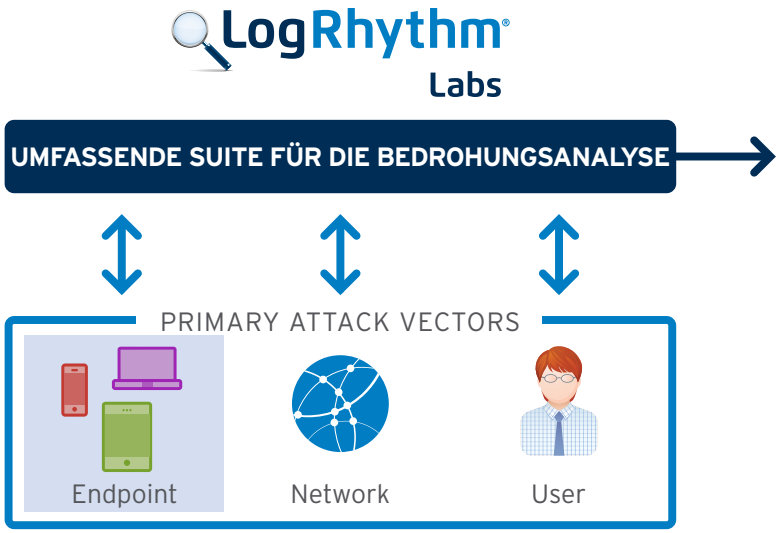
Funktionsweise

Die Endpoint Threat Analytics Suite analysiert die vorhandenen Logdaten der Hosts sowie die Daten, die LogRhythms System Monitors von sammeln. Die AI Engine nutzt hierbei ein umfassendes Regelset für die Verhaltensanalysen, um die Angriffe auf die Endpunkte eines Unternehmens zu erkennen, zu priorisieren und zu eliminieren. Neben der Erkennung von Malware-Aktivitäten und gefährlichen Verhaltensmustern, die mit Zero-Day-Attacken einhergehen, kann die Endpoint Threat Analytics Suite auch nicht autorisierte lokale Benutzerkonten, Fehlkonfigurationen, den Missbrauch von privilegierten Zugangsdaten sowie die Kompromittierung von Endpunkten aufdecken. Mit der Suite erhalten Kunden auch einen verständlichen Leitfaden für die Implementierung mit Empfehlungen zu Konfigurationen und für das Setup, sodass sie bewährte Methoden nutzen und einen schnellen ROI erzielen können.

Schädliche Software
- Malware-Ausbruch
- Anormale Prozessaktivität
- Neuer Autorun-Prozess
- Neue Softwareinstallation
- Lokale Einschränkungen der Sicherheit

Zugriffsversuche auf Hosts
- Pass-the-Hash (Erweiterte Passwort-Attacken)
- Ausführung der PowerShell
- Erstellung und Nutzung eineslokalen Benutzerkontos
- Mehrere fehlgeschlagene Zugriffsversuche

Windows Firewall-Ereignisse
- Mehrere Änderungen an der Firewall
- Prozess wird der Firewall hinzugefügt
- Firewall-Regel hinzugefügt/ modifiziert
- Sicherheitsereignis und Änderung der Firewall



Die hohe Anzahl an Endpunktgeräten in einem Unternehmensnetzwerk, von denen jedes einzelne einen möglichen Angriffspunkt darstellt, schafft eine Fülle an Sicherheitslücken im Netzwerk eines jeden Unternehmens. Die Endpoint Threat Analytics Suite von LogRhythm verfolgt einen ganzheitlichen Ansatz zur Überwachung und Analyse des Endpunktverhaltens in Echtzeit und nutzt hierfür eine Reihe von Verfahren zum Schutz des Netzwerks vor Angriffen an den Endpunkten. Die Lösung unterstützt Unternehmen dabei, die sicherheitsrelevanten Ereignisse zu ermitteln, die Aktivitäten nach ihrer Bedeutung zu priorisieren und automatisierte Maßnahmen zur Abwehr der Bedrohungen einzuleiten - noch bevor diese erheblichen Schaden anrichten.

Manipulation der Endpunkte: Haben Angreifer erst einmal einen Endpunkt kompromittiert, nutzen sie ihn als Ausgangspunkt, um Software zu installieren, die automatisiertschädliche Aktivitäten ausführt. Die Endpoint Threat Analytics Suite setzt eine Reihe von Verfahren ein, um Aktivitäten zu erkennen, die entweder auf einen externer Angreifer hinweisen, der denSchutz am Netzwerk-Perimeter durchbrochen hat, oder auf einen böswilligen Insider, der von innen angreift. Diese Verfahren umfassen vordefinierte Regeln für die Verhaltensanalyse, die Sicherheitsverantwortliche auf ungewöhnliche Aktivitäten am Endpunkt hinweist, wie etwa nicht autorisierte Softwareinstallationen, neue Autorun-Prozesse oder verdächtige PowerShell-Aktivitäten in Verbindung mit Schadprogrammen. Alle Alarme ermöglichen einen sofortigen Drill-Down auf alle forensischen Daten für eine schnelle Problembehebung.

Änderungen der Systemkonfiguration: Angreifer führen Konfigurationsänderungen an den Endpunkten durch und ermöglichen es damit, dass sich Malware im gesamten Firmennetzwerk verbreitet und so Schaden anrichten kann. Die Endpoint Threat Analytics Suite von LogRhythm nutzt eine Reihe von Techniken, um diese Änderungen an den Endpunkten zu erkennen und fordert Sicherheitsverantwortliche zu weiteren Untersuchungen auf. Die Lösung bietet zahlreiche vordefinierte Regeln, die Änderungen an Host-Firewalls, in Verzeichnisdiensten, in der Windows-Registry, Netzwerkzugängen und in den Überwachungsprozessen des Hosts in Echtzeit feststellen können. Diese Ereignisse werden automatisch mit den vorhandenen, umfassenden Benutzer- und Netzwerkdaten in Beziehung gesetzt, um Ausgangspunkt der Aktivität zu bestimmen und das Problem schnell beheben zu können.

Kommunikation mit verdächtigen IP-Adressen: Netzwerkkommunikation mit verdächtigen IP-Adressen und IP-Adressbereichen ist ein sehr guter Indikator für einen Malware-Ausbruch oder eine erfolgreich durchgeführte Sicherheitsverletzung eines Angreifers. Doch viele Unternehmen haben keine Möglichkeit, automatisch zu erkennen, ob verdächtiger Datenverkehr mit Cyber-Kriminellen und Angreifern in Verbindung gebracht werden kann. Die Network Threat Analytics Suite von LogRhythm umfasst zahlreiche, vordefinierte Regeln, die verdächtige Netzwerkaktivitäten erkennen und diese Daten automatisch mit den Threat Intelligence-Daten abgleichen, die das LogRhythm Threat Intelligence Ecosystem liefert. Diese Regeln treten je nach Bedrohlichkeit der Aktivitäten automatisch in Kraft. Dies umfasst auch die gesamte Netzwerkkommunikation mit Standorten, die auf der Blacklist oder der Whitelist stehen.

Überwachung der Firewall: Schadprogramme sind häufig darauf ausgerichtet, dass sie verdeckt Kommunikationswege zu einem externen Ziel öffnen, wie etwa zu einem Command-and-Control-System, um einen dauerhaften Angriffspunkt für kontinuierliche, schadhafte Aktivitäten zu schaffen. Die Endpoint Threat Analytics Suite von LogRhythm bietet spezielle Regeln, um zu erkennen, ob einer Firewall neue Prozesse hinzugefügt wurden oder die Konfiguration der Firewall (Hinzufügen, Bearbeiten oder Löschen bestehender Regeln) geändert wurde. Dabei werden auch weitere Informationen wie andere verdächtige Ereignissen oder eine hohe Zahl an Firewall-Änderungen innerhalb kurzer Zeit, etc. einbezogen. Nicht autorisierte Änderungen der Firewall-Konfiguration sind ein deutlicher Hinweise auf eine Kompromittierung und ermöglichen es IT-Verantwortlichen, schnell auf Sicherheitsverletztungen an den Endpunkten zu reagieren noch bevor diese Schaden anrichten können.

Malware-Aktivitäten: Schadprogramme sind häufig so konzipiert, dass sie ihre Spuren verwischen, indem Prozessaktivitäten nicht aufgezeichnet oder Änderungsprotokolle nach begangener Tat modifiziert werden. Die Endpoint Threat Analytics Suite nutzt die vorhandenen forensischen Daten des Endpoint Monitors von LogRhythm, um Schadprogramme zu erkennen, die auf herkömmlichem Weg nicht erkannt werden, bevor sie größeren Schaden anrichten können. Die Suite umfasst mehrere Regeln, die Sicherheitsverantwortliche von ungewöhnlichen Softwareaktivitäten in Kenntnis setzen. Hierzu zählenProzesse, die nicht auf der Whitelist stehen und von einem Endpunkt ausgehen. Zusätzliche Informationen, die auf kritische oder angreifbare Endpunkte hinweisen, reduzieren die Anzahl der „False-Positives“ (Fehlalarme) und priorisieren die Ereignisse automatisch. Das vorkonfigurierte Plug-In SmartResponse kann jeden nicht autorisierten Prozess sofort stoppen, bevor er Schaden anrichtet.