PRODUKTÜBERSICHT

Core Threat Analytics Suite

LogRhythm
The Security Intelligence Company

Die heutigen Cyber-Bedrohungen werden immer komplexer und ausgeklügelter und setzen Unternehmen verstärkt dem Risiko schädigender Angriffe und Sicherheitsverletzungen aus. Obwohl die meisten Unternehmen sich der steigenden Gefahr durch Angriffe bewusst sind, verfügen sie oftmals nicht über ausreichend personelle Ressourcen oder das notwendige Knwo-how und die passenden Tools, um Cyber-Bedrohungen effektiv zu bekämpfen. Der Aufbau einer effektiven und modernen Sicherheitsinfrastruktur erfordert einen ganzheitlichen Security Intelligence-Ansatz, um Cyber-Bedrohungen innerhalb und außerhalb eines Netzwerks erkennen, priorisieren und eliminieren zu können . Vollkommene Transparenz in Echtzeit sowie ein tiefgehendes Verständnis für die Bedrohungen, die die gesamte Angriffsfläche (Endpunkte, Netzwerke, User) betreffen, sind die Voraussetzungen hierfür.

Analysen gegen zentrale Bedrohungen

- ✓ schneller Einsatz, minimale Konfiguration
- ✓ Transparenz in Bezug auf Endpunkte, Netzwerk und User
- ✓ automatisierte Gefahrenanalyse
- ✓ Ausrüstung mit bewährten Sicherheitsverfahren

Die Core Threat Analytics Suite von LogRhythm unterstützt Unternehmen dabei, die operationalen und technische Hindernisse zu überwinden. Die Lösung stellt automatisierte Funktionen Out-of-the-Box zur Verfügung, die die Erkennungs- und Reaktionszeit auf eine Vielzahl an Cyber-Bedrohungen reduzieren. Die LogRhythm Labs haben die Suite entwickelt, um Verhaltensanalysen über die User-, Endpunkt-, Netzwerkaktivitäten schnell und effizient bereitzustellen und so den Schutz vor allen geläufigen Angriffsvektoren zu gewährleisten. Die Suite kann alle herkömmlichen Logdaten, die in den IT-Infrastrukturen der Unternehmen entstehen, verarbeiten. Hierzu zählen die Daten des Active Directory/LDAP, von Antiviren-/Anti-Malware-Lösungen, der Firewalls, der Hosts, von IDS/IPS-Systemen und VPN-Lösungen sowie Netzwerkflussdaten.

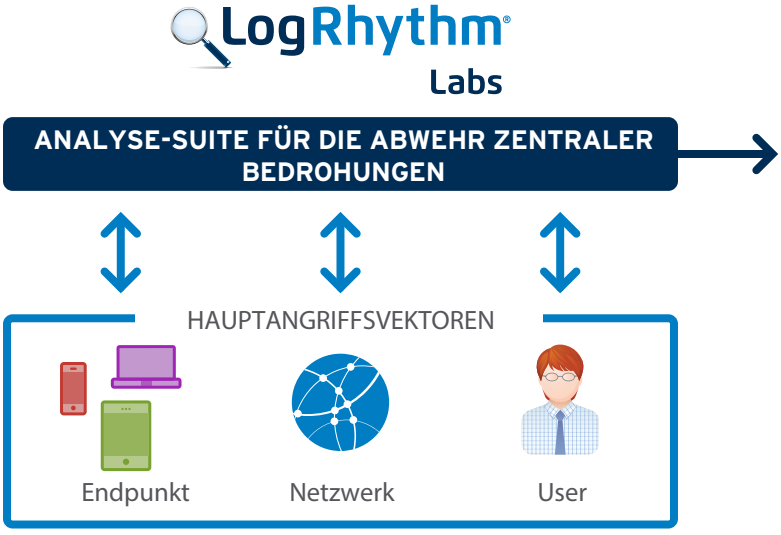
Funktionsweise

Die Core Threat Analytics Suite nutzt die AI Engine von LogRhythm, die eine umfassende Sammlung automatisierter Regeln für die Maschinenanalyse bereitstellt, die lediglich eine minimale Konfiguration erfordern. Diese Regeln nutzen eine Reihe von Verfahren für die Bedrohungserkennung, einschließlich hoch entwickelter Korrelation, Mustererkennung, Blacklisting und Whitelisting sowie statistischer Analyse. Unternehmen können das Modul unmittelbar einsetzen und konfigurieren, um nach Anomalien, die mit Endpunkt-, Netzwerk- und Nutzeraktivitäten verbunden sind, zu suchen. 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..

Endpunkte
Verdächtige Konfigurationsänderungen
Fehlgeschlagene Malware-Säuberung
Unerlaubte Änderung des Audit-Protokolls
Durch einen Angriff entstehender Schaden
und mehr...

Netzwerke
Brute-Force-Angriffe
Malware-Ausbrüche
Verdächtige Netzwerkaktivitäten
Verdächtiges Verhalten ähnlich dem Anfangsstadium eines Angriffs
und mehr...

User
Kompromittierung von Benutzerkonten
Verdächtige Aktivitäten der BenutzerkontenKonto
Durchdringung des Netzwerks
Missbrauch privilegierter Benutzerrechte
und mehr...



Die Großzahl erfolgreicher Angriffe und Sicherheitsverletzungen nutzt kompromittierte oder gestohlene Benutzerdaten, greift Endpunkte mit Malware an oder dringt mit Zero-Day- oder zielgerichteten Angriffen am Netzwerk-Perimeter ein. Die Core Threat Analytics Suite verfolgt einen ganzheitlichen Ansatz des Netzwerkschutzes, indem sie alle drei Hauptangriffsvektoren mit einer Reihe von Verfahren in Echtzeit überwachen. Die Suite ermittelt das sicherheitsrelevante, ursprüngliche Ereignis, priorisiert die Bedrohungen nach ihrer Gefährdung für das Unternehmen und leitet automatisiert Gegenmaßnahmen ein, um den Angriff zu eliminieren, noch bevor dieser Schaden anrichten kann.

Malware-Ausbruch: Hostbasierende Antivirenlösungen können einzelne Malware-Vorfälle gut erkennen, aber nicht immer können sie Ausbrüche, die mehrere Endpunkte betreffen, identifizieren und den Ausgangspunkt des Malware-Ausbruchs finden. Die Regeln der Core Threat Analytics Suite erkennen einen Ausbruch automatisch, indem sie die Logdaten der bestehenden Antivirenlösungen, die in den meisten IT-Umgebungen eingesetzt werden , in Korrelation zueinander setzen. Unternehmen können sich alle Informationen hierzu auch im Detail ansehen, um alle infizierten Systeme und den eigentlichen Ausgangspunkt des Malware-Ausbruchs zu ermitteln. Das Plug-In SmartResponse kann infizierte Geräte unter Quarantäne stellen und so die Bedrohung unverzüglich neutralisieren.

Datenausschleusung: Da die Bedrohungen durch die eignen Mitarbeiter im Unternehmen oftmals als rechtmäßige Aktivitäten erscheinen werden sie von herkömmlichen Sicherheitslösungen häufig erst in einer späten Phase des Angriffs erkannt. Deshalb ist es umso wichtiger, den Angriff sofort zu stoppen und den Schaden, der bis zu diesem Zeitpunkt des Angriffs bereits entstanden ist, möglichst zu minimieren Die Regeln der Core Threat Analytics Suite können die unmittelbar verfügbaren Logdaten von Hostsystemen sowie Geräten für die Sicherheits- und Netzwerküberwachung nutzen und das Angriffsverhalten zu spezifischen Maßnahmen in Beziehung setzen. So können sie auch erkennen, ob weitere schadhafte Aktivitäten wie Datenausschleusung stattfinden. Unternehmen können definieren, wie sie ihre Reaktionmaßnahmen auf die Ereignisse priorisieren möchten. So können sie die Aktivitäten, die das höchste Risiko bergen, zuerst zu untersuchen, während SmartResponse die Bedrohung automatisch eliminieren kann, indem das Benutzerkonto deaktiviert oder die Quell-IP-Adresse blockiert werden.

Kompromittierte Benutzerkonten: Kompromittierte Zugangsdaten sind eine weit verbreitete Methode, mit der Angreifer erfolgreich in Netzwerke eindringen. Jedoch ist es ohne geeignete Tools und Expertenwissen sehr schwer zu erkennen, ob Zugangsdaten gestohlen wurden und ob diese für einen Angriff verwendet werden. Die Core Threat Analytics Suite bietet vorkonfigurierte Regeln, die die Authetifizierungsaktivitäten, die in den Active Directory/LDAP-Logs aufgezeichnet werden, mit den Angriffsdaten, die eine IDS/IPS-Lösung liefert, in Korrelation zueinander setzt, um zu erkennen, ob die Benutzerdaten für einen Angriff genutzt wurden.. SmartResponse kann ein auffälliges Benutzerkonto entweder sofort deaktivieren oder es einer Merkliste hinzufügen, um höher priorisierte Warnmeldungen auszulösen, falls weitere verdächtige Aktivitäten in Zusammenhang mit diesem Benutzerkonto auftreten.

Missbrauch von Benutzerrechten: Der Missbrauch privilegierter Konten kann in einem Unternehmen erheblichen Schaden anrichten – ganz gleich, ob dieser von böswilligen Insidern oder externen Angreifern ausgeht. So können gestohlene Administrationsrechte für eine Vielzahl schädlicher Aktivitäten verwendet werden wie beispielsweise die Lösung oder der Diebstahl von geschäftskritischen Daten oder die Neukonfiguration der Sicherheitseinstellungen, wodurch das Netzwerk dann weiteren Angriffen ausgesetzt ist.Die Core Threat Analytics Suite unterstützt bewährte Vorgehensweisen, überwacht Active Directory- bzw. LDAP-Logs, und meldet beispielsweise, wenn ein Konto zu einer administrativen Gruppe hinzugefügt wird. Die Lösung kann dies automatisch mit einer Whitelist berechtigter privilegierter User abgleichen, um potenziellen Missbrauch aufzudecken. SmartResponse kann bis zum entsprechenden Nachweis automatisch jedes Konto deaktivieren, dem unerlaubte Zugriffsrechte gewährt wurden.

Kompromittierte Server: IDS/IPS-Lösungen generieren typischerweise eine so große Menge an Ereignissen, dass die Unterscheidung zwischen False-Positives (Fehlalarmen) und wirklichen Angriffen, die sofortige Beachtung verdienen, schwierig ist. Die Core Threat Analytics Suite untersucht IDS/IPS-Ereignisse, Logdaten von Firewalls und Flussdaten, um sicherheitsrelevante Ereignisse zu Netzwerkaktivitäten in Beziehung zu setzen und so beispielsweise zu erkennen, ob ein angegriffenes Hostsystem möglicherweise einen besonders schädlichen Payload empfangen hat. Unternehmen mit zusätzlichen Netzwerksensoren wie Firewalls der nächsten Generation oder dem LogRhythm Netzwerk Monitor können noch detailliertere Informationen auf Datenpaket-Ebene nutzen, um die Genauigkeit zusätzlich zu erhöhen.SmartResponse kann die Bedrohung automatisch eliminieren, indem das Tool den kompromittierten Server in Quarantäne nimmt.