PRODUKTÜBERSICHT

Endpunktüberwachung und -forensik

LogRhythm
The Security Intelligence Company

Der Schutz Ihres Unternehmens vor komplexen Bedrohungen, Compliance-Verletzungen und betrieblichen Problemen ist ein fortlaufender Prozess. Er erfordert hohe Transparenz, ständige Überwachung, automatisierte Verhaltensanalysen, fortschrittliche Bedrohungserkennung, intelligente Abwehrfähigkeiten und die kontinuierliche Anpassung an neue, sich ständig weiterentwickelnde Probleme und Bedrohungen. Eine Hauptkomponente dieses Prozesses ist die Fähigkeit, die Geschehnisse auf der Endpunkt-Ebene mit den Ereignisdaten innerhalb des Netzwerks abgleichen zu können. LogRhythm bietet umfangreiche Transparenz und erweiterten Schutz durch eine vollständige integrierte Endpunktüberwachung und -forensik.

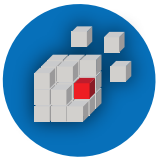
Die Korrelation von Ereignisdaten aus dem gesamten Netzwerk mit den Aktivitäten auf den Endpunkten wird oftmals dadurch behindert, dass wichtige Endpunkt-basierte Aktivitäten nicht fortlaufend aufgezeichnet werden und häufig mehrere Lösungen benötigt werden, um diese Informationslücken zu schließen. Die Endpunktüberwachung und -forensik liefert eigenständige Erkenntnisse zu den Geschehnissen an einem Endpunkt und bietet damit einen wichtigen zusätzlichen Schutz vor einem breiten Spektrum an Problemen. Diese reichen von gravierenden betrieblichen Ereignissen wie System- und Anwendungsausfällen bis hin zu Sicherheits- und Compliance-Verletzungen, die auf unerlaubte oder böswillige Aktivitäten zurückzuführen sind.

Endpoint Monitoring and Forensics ist eine zentral überwachte und verwaltete Komponente, die vollständig in LogRhythm integriert ist. Sie bietet:

- Unabhängige Aufzeichnung wichtiger Endpunkt-Aktivitäten
- Erkennen von Änderungen an der Startregistrierung von Windows
- Umfassende Ereignisdetails
- Schutz vor Zero-Day-Angriffen und kritischen Fehlern
- Schutz vor unerlaubten Datentransfers
- Vollständige Integration mit allen Ereignisdaten für eine starke Korrelation und Ereigniszusammenhänge

Unabhängige Prozessüberwachung

Die Lösung erkennt Prozess- und Service-Aktivitäten, die sonst möglicherweise nicht festgehalten würden, und zeichnet sie auf. Auf diese Weise können kritische Verhaltensweisen aufgedeckt und entsprechende Alarme ausgegeben werden: zum Beispiel, wenn Endpunkte verbotene Prozesse ausführen (Peer-to-Peer-Clients etc.), wenn wichtige Prozesse angehalten oder nicht genehmigte Prozesse gestartet werden.



Überwachung der Windows-Registrierung

Überwacht, ob Zusätze, Änderungen, Löschungen, Berechtigungsänderungen (ACL) oder Eigentümerwechsel an der Registrierung von Windows vorgenommen werden. Dies erleichtert den Einblick in Änderungen oder Manipulationen am Windows-Betriebssystem, wie z.B. das Hinzufügen neuer Startvorgänge, und damit die Erkennung fortgeschrittener Bedrohungen und gefährdeter Endpunkte.

Überwachung der Netzwerkverbindung

Protokolliert selbstständig die Netzwerkverbindungen zum und vom Endpunkt und bietet somit ein detailliertes, unabhängiges Protokoll aller Netzwerkverbindungen, die an einem Endpunkt geöffnet und geschlossen werden. Kritische Ereignisse am Endpunkt, wie z.B. Aktivitäten unautorisierter Web- oder FTP-Server, werden entdeckt und gemeldet.

Data Loss Defender

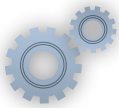
Überwacht und schützt Datentransfers zu und von Wechseldatenträgern wie CD-/DVD-RW-Geräten oder USB-Laufwerken. Data Loss Defender protokolliert, meldet und prüft alle Datentransfers zu Anschlüssen von Wechseldatenträgern und kann optional Transfers auf bestimmte Maschinen und Geräte blockieren.

Überwachung der Benutzeraktivität

Protokolliert jeden Benutzer oder Prozess, der sich bei einem Endpunkt authentifiziert. Legt selbstständig einen Prüfpfad an, der verwendet werden kann, um lokale Prüfsysteme zu unterstützen oder sicherzustellen, dass keine Systemprotokolle am Endpunkt verändert wurden.

Die Kombination aus LogRhythm Endpoint Monitoring and Forensics und der umfassenden Security Intelligence-Plattform von LogRhythm ermöglicht einzigartige Einblicke in die Abläufe innerhalb der IT-Umgebung. Mithilfe der leistungsstarken Smart**Response**™-Technologie bietet LogRhythm umfassenden, aktiven Schutz vor komplexen Bedrohungen, Compliance-Verletzungen und betrieblichen Fehlern auf der Endpunkt-Ebene.

Unabhängige Prozessüberwachung

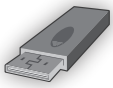


Problem In den IT-Systemen von Unternehmen werden ständig Prozesse gestartet und angehalten, aber nicht ausreichend protokolliert. Ohne eine unabhängige Aufzeichnung aller Ereignisse ist es jedoch sehr schwierig, einzelne Ereignisse zu erkennen, wie etwa, ob wichtige Prozesse nach einer Routinewartung korrekt neu gestartet werden.

Entdeckung LogRhythm kann selbstständig erkennen und melden, wenn ein auf der schwarzen Liste aufgeführter Prozess gestartet wird, ein wichtiger Prozess stoppt oder ein kritischer Prozess nach einem bestimmten Ereignis nicht mehr anläuft, zum Beispiel nach einem Neustart.

Behebung Smart**Response**™ kann individuelle Vorgänge anhalten und/oder starten und bezieht dabei alle relevanten Informationen, wie den Prozessnamen und den betroffenen Endpunkt, direkt aus dem Alarm.

Data Loss Defender



Problem Bei vielen komplexen Bedrohungen, die zu Datenschutzverletzungen führen, werden physische Mittel wie Wechseldatenträger (z.B. USB-Laufwerke und CD-/DVD-RW-Geräte) verwendet, um sensible Daten aus dem Netzwerk zu beziehen.

Erkennung LogRhythm kann selbstständig die Verwendung von Wechseldatenträgern direkt am Endpunkt erkennen und generiert einen Alarm, bevor Daten auf einen oder von einem Wechseldatenträger übertragen werden.

Behebung Data Loss Defender kann den Transfer auf bzw. von Wechseldatenträgern automatisch verhindern, indem das Gerät sofort ausgeworfen oder deinstalliert wird.

Überwachung der Windows-Registrierung

Problem Änderungen an der Registrierung von Windows werden nativ nicht protokolliert, sodass es schwierig ist, Änderungen wie das Hinzufügen schädlicher Software zu entdecken. Hat sich eine Malware erst einmal in der Registry festgesetzt, kann sie sich leicht ausbreiten, indem sie Prozesse steuert, Nutzdaten herunterlädt und weitere Systeme infiziert.

Erkennung LogRhythm kann die Windows Registry selbstständig überwachen, um Änderungen zu ermitteln, wie etwa die Einschleusung böswilliger Software und die Einführung neuer Startvorgänge.

Behebung Wenn Änderungen an der Registrierung entdeckt werden, alarmiert LogRhythm das IT- und Sicherheitspersonal. Wird eine Änderung als schädlich erkannt, können die Administratoren ein Smart**Response**™ Plug-In autorisieren, das die Startvorgänge deaktiviert, um die Verbreitung von Malware zu verhindern.

Überwachung der Netzwerkverbindung

Problem Detaillierte Informationen über das Netzwerkverhalten auf der Endpunkt-Ebene sind eine wichtige Komponente der Echtzeit-Überwachung und forensischen Analyse. Sie zu gewinnen kann jedoch schwierig sein, wenn verbindungsspezifische Protokolldaten fehlen oder der Zugriff auf den Datenfluss eingeschränkt ist.

Erkennung LogRhythm erstellt ein unabhängiges Protokoll jeder Netzwerkverbindung an einem überwachten Endpunkt. Dieses zeigt relevante Details wie die Port-ID, die Kommunikationsrichtung und den Prozess, mit dem die Verbindung geöffnet wurde.

Behebung Smart**Response**™ kann so konfiguriert werden, dass in Reaktion auf einen Alarm ein unerlaubter Port geschlossen oder eine verdächtige Netzwerkverbindung beendet wird.

Überwachung der Benutzeraktivität

Problem Um spezifische Ereignisse umfassend verstehen zu können, ist es enorm wichtig zu wissen, wer an einem bestimmten Endpunkt angemeldet ist, wenn böswillige Aktivitäten ausgeführt werden oder kritische betriebliche Vorgänge fehlschlagen.

Erkennung LogRhythm kann selbstständig protokollieren, wer wie lange angemeldet ist, und gleicht Aktivitäten zur Benutzerprüfung mit anderen Protokoll- und Ereignisdaten ab, sodass eine umfassende Prüfung des Benutzerverhaltens innerhalb der IT-Umgebung durchgeführt wird.

Behebung Smart**Response**™ kann Benutzerkonten mit verdächtigem Verhalten automatisch deaktivieren oder optional einen Genehmigungsprozess einleiten.

Sperren eines Endpunkts

Problem Selbst nachdem eine Gefährdung entdeckt wurde, arbeiten die Geräte in einem Netzwerk weiter. Auf diese Weise kann schädliche Software in das Unternehmen eindringen, sich auf andere Systeme ausbreiten und immer mehr Zugriff auf Netzwerkressourcen erhalten.

Erkennung Smart**Response**™ kann automatisch eine Reihe von Scans direkt auf dem Host durchführen, um eine umfassende Diagnose und forensische Daten für eine exakte Analyse der Ursache zu erstellen.

Behebung Smart**Response**™ kann den Geräte- und Benutzerzugriff auf andere Ressourcen automatisch deaktivieren, damit ein kompromittierter Host keine anderen Geräte im Netzwerk infizieren kann.