PRODUKTÜBERSICHT

SmartResponse™ Automation Framework

LogRhythm
The Security Intelligence Company

Vorfallsreaktion in Sekunden, nicht erst in Tagen

Wenn ein Unternehmen eine Gefährdung in seinem Netzwerk entdeckt, kann eine schnelle Reaktion auf Ereignisse entscheidend dafür sein, ob die Bedrohung eingedämmt werden kann oder zu einer gravierenden Datenpanne wird. Unternehmen, die sich ausschließlich auf manuelle Verfahren verlassen, haben Schwierigkeiten, die Reaktionszeiten zu verringern, und sind einem höheren Risiko ausgesetzt. Firmen, die ihre Reaktionszeiten verbessern möchten, sollten die allgemeine Untersuchung und die Behebungsmaßnahmen automatisieren.

Leider war eine Automatisierung für die meisten Unternehmen bislang nicht machbar. Die Entwicklung einer eigenen Lösung ist in der Regel unerschwinglich teuer, und vorhandene kommerzielle Optionen sind entweder unflexibel oder erfordern aufwändige und kostenintensive Anpassungen.

Ein effektives Automatisierungswerkzeug muss folgende Anforderungen erfüllen:

- Effiziente Workflows und flexible Genehmigungsprozesse
- Unkomplizierte Integration in die IT-Umgebung
- Unterstützung für mehrere Betriebssysteme
- Möglichkeit des Transfers innerhalb getrennter Netzwerke
- Integrierte Überprüfung
- Minimale Kosten und Komplexität

Eine automatisierte Problembehebung, die funktioniert

Smart**Response**™ ist eine einzigartige Lösung zur automatisierten Reaktion auf Ereignisse. Zudem ermöglicht die Software auch einen halbautomatischen, genehmigungsbasierten Betrieb, sodass Benutzer die Situation prüfen können, bevor Gegenmaßnahmen durchgeführt werden.

LogRhythm reduziert die Zeit, die für die allgemeine Untersuchung und die Abwehrmaßnahmen benötigt wird, und verhindert auf diese Weise die rasante Verbreitung von Gefährdungen mit hohem Risikopotenzial. Beispiele hierfür sind die Aktivierung eines Schwachstellenscans bei einem verdächtigen Endpunkt oder drastischere Maßnahmen wie die Quarantäne eines gefährdeten Endpunkts oder die Deaktivierung eines verdächtigen Benutzerkontos.

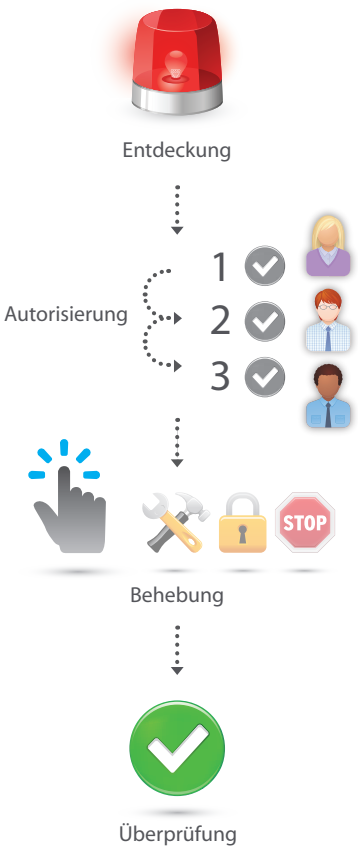
Vorgefertigte und kundenspezifische Plug-Ins

LogRhythm Labs bietet Kunden eine umfangreiche Bibliothek an vorgefertigten Smart**Response**-Maßnahmen. Zudem hilft LogRhythm den Anwendern, benutzerdefinierte Plug-Ins mit dem Programm bzw. der Scripting-Technologie ihrer Wahl zu erstellen, wie z.B. Bash, Java, .NET, Perl, PowerShell oder Python. Die Benutzer können eigene Plug-Ins mit einem integrierten Tool testen, das die Ausgabe dokumentiert und Fehler identifiziert. Mit den vorgefertigten und benutzerdefinierten Smart**Response**-Maßnahmen erhält der Kunde die Kontrolle.

Alarmintegration

Das Smart**Response** Automation Framework ist eng in die LogRhythm-Plattform integriert. Dadurch bietet es nahtlose Kontinuität, von der durchgehenden Bedrohungserkennung bis hin zu den Abläufen zur Behebung von Störungen.

Die Benutzer legen Smart**Response**-Aktionen fest, die durch bestimmte Alarme ausgelöst werden. Diese Alarme können Daten an die Smart**Response**-Aktion weiterleiten und ermöglichen somit eine dynamische, präzise Ausführung. Ein einziger Alarm kann mehrere Smart**Response**-Aktionen auslösen, sodass Untersuchungs- und Abwehrmaßnahmen gleichzeitig durchgeführt werden können.



Differenzierte Genehmigungsverfahren

In bestimmten Fällen kann es sinnvoll sein, dass SmartResponse erst aktiv wird, wenn die Maßnahmen durch einen Notfallmanager oder mittels formeller Freigabeprozesse überprüft werden können. Mit Smart**Response** können die Benutzer differenzierte Genehmigungsszenarien als Vorbedingung für die Ausführung der Maßnahmen implementieren. Zudem unterstützt LogRhythm komplexe Genehmigungsketten, einschließlich Genehmigungen durch mehrere verschiedene Gruppen, wenn unternehmensübergreifende Freigaben erforderlich sind.

Flexible Ausführungsmöglichkeiten

Das LogRhythm Smart**Response** Automation Framework unterstützt mehrere Optionen für die Ausführung von Maßnahmen:

- **Ausführung der gesamten Maßnahmenkette:** Konfigurieren Sie SmartResponse so, dass alle Maßnahmen ohne Freigabe vollautomatisiert durchgeführt werden. Dies beschleunigt die Eindämmung von Gefährdungen, und Bedrohungen mit hohem Risikopotenzial werden in Sekunden neutralisiert.
- **Ausführung mit einem Klick:** Führen Sie eine Maßnahme manuell durch. Das LogRhythm Smart**Response** Automation Framework erlaubt eine unmittelbare Ausführung von Maßnahmen mit nur einem Klick auf die LogRhythm-Benutzeroberfläche.
- **Remote-Ausführung von System Monitor:** Leiten Sie Maßnahmen über unterschiedliche Netzwerke an Remote-Standorten ein, auf die nicht direkt per IP-Routing zugegriffen werden kann. Smart**Response** ermöglicht dies durch Maßnahmen, die an System Monitor-Agenten übertragen und lokal ausgeführt werden können. Auf diese Weise unterstützt Smart**Response** eine globale, verteilte Störungsbehebung.

Vollständige Prüfung und Erfüllung der Rechenschaftspflicht

Zur Reaktion auf ein Ereignis werden häufig viele verschiedene Personen, Teams und Technologien benötigt. Mit Smart**Response** verfolgt und protokolliert LogRhythm alle Aktivitäten, die zur Eindämmung und Abwehr der Gefährdung durchgeführt werden. Auf diese Weise entfällt der Arbeitsaufwand für die manuelle Aufzeichnung und Konsolidierung von Informationen zur Störungsbehebung, einschließlich Genehmigungen und Mitteilungen. Die Aufzeichnung von Prüfpfaden hilft Unternehmen, den Prozess der Störungsbehebung zu optimieren, mit dem Management zu kommunizieren und alle Compliance-Anforderungen einzuhalten.

Maximale Nutzung vorhandener Investitionen

Das LogRhythm Smart**Response** Automation Framework kann leicht in aktuelle und künftige Sicherheitstechnologien integriert werden. Dank der umfassenden Herstellerunterstützung können die Benutzer im gesamten Netz reagieren, unabhängig davon, welche Sicherheitstools, IT-Infrastrukturen, Netzwerktechnologien, Systeme und Anwendungen sie einsetzen.

Anwendungsfälle

Die Teams, die für die Reaktion auf ein Ereignis zuständig sind, werden mit vorgefertigten und individualisierbaren Plug-Ins ausgerüstet, wodurch die Reaktionszeit von Tagen auf Minuten verkürzt werden kann. Beispiele für Smart**Response**-Anwendungsfälle:

- **Endpunkt-Quarantäne:** Identifizieren Sie den Netzwerkanschluss, an dem sich ein verdächtiges Gerät befindet, und deaktivieren Sie den Anschluss/das Gerät.
- **Benutzer sperren:** Sperren Sie unabhängig von dem verwendeten Gerät den Zugriff auf ein Benutzerkonto, wenn der Verdacht besteht, dass ein Konto kompromittiert ist.
- **Maschinendaten sammeln:** Im Falle von Malware-Infektionen können forensische Daten vom verdächtigen Endpunkt gesammelt werden.
- **Netzwerkzugriff sperren:** Wenn Daten ausgeschleust werden, kann das für die Störungsbehebung zuständige Team die Zugriffskontrolllisten der Firmen-Firewalls aktualisieren und so die Verbindung trennen.
- **Prozesse beenden:** Wenn ein Team unbekannte oder auf der schwarzen Liste aufgeführte Vorgänge auf wichtigen Geräten entdeckt, kann Smart**Response** das betreffende laufende Programm beenden.