AIE Visual Aid

AIE Rules Represented Visually

4/27/2018

LogRhythm Inc.

4780 Pearl East Circle

Boulder, CO 80301

(303) 413-8745

www.logrhythm.com

LogRhythm Customer Support

support@logrhythm.com

Contents

Overview

This document provides an alternative method to build AIE rules visually. This covers many of the rule blocks and covers what items are listed for each rule that have to be determined. This visual aid does not cover the Whitelist and Trend rule blocks.

AIE Visual Aid

Traditional Alarm

Common Event = AD Sync Error	**Primary**
	Include
	Exclude
Host Impacted = Server X	**Group By**
Common Event = AD Sync Error	**Group By**
Count = 20	**Measurement (Aggregation)**
Past 10 minutes	**Live Time (Time Limit)**
Every 1 Sec	**Evaluation Frequency**
Expression: Common Event Log Count >=20	

Log Observed Rule Block

Log Observed	**Rule Block**	Log Not Observed Compound
Common Event = Service Stopped	**Primary**	Common Event = Service Started
	Include	
	Exclude	
Process Name = AV service	**Group By**	Process Name = AV service
Host Origin = Server A	**Group By**	Host Origin = Server A
Count = 1	**Measurement (Log Count)**	Count = 1
0	**Live Time (Time Limit)**	
Every 1 Sec	**Evaluation Frequency**	
	Relationship Time	
Expression: Classification Log Count = 1	1 hour	Expression: Classification Log Count = 1

Threshold Rule Block

Log Observed	**Rule Block**	Threshold Observed
Common Event = FIM access granted	**Primary**	Host Impacted KB received = not nothing
	Include	direction = outbound
	Exclude	
Host Origin = 10.10.10.101	**Group By**	Host Impacted = 10.10.10.101
Host impacted = Server X	**Group By**	Host Origin = Server X
Count = 1	**Measurement (bytes)**	Host Impacted KB received >= 5MB
0	**Live Time (Time Limit)**	1 day
Every 1 Sec	**Evaluation Frequency**	Every 1 Sec
	Relationship Time	
Expression: Classification Log Count = 1	1 hour	Expression = Host Impacted KB Received >= 5MB

Unique Value Rule Block

Rule Block	Unique Value Not Observed Scheduled	Unique Value Not Observed Scheduled	Unique Value Not Observed Scheduled
Primary	Common Event = backup complete	Common Event = backup complete	Common Event = backup complete
Include			
Exclude			
Group By			
Group By	Common Event = backup complete	Common Event = backup complete	Common Event = backup complete
Unique Value (Host Impacted)	Host Impacted = Server A	Host Impacted = Server B	Host Impacted = Server C
Measurement (Occurrence)	Classification Log Count = 3		
Live Time (Time Limit)	Past 10 minutes		
Evaluation Frequency	Every 1 Sec		
Relationship Time			
N/A	Expression: Impacted User Unique >= 3		

Statistical Rule Block (Behavioral)

Rule Block	Statistical (Unique Value)	Statistical (Unique Value)	Statistical (Unique Value)	Statistical (Threshold)
Primary	Classification = Authentication Failure	Classification = Authentication Failure	Classification = Authentication Failure	Classification = Authentication Failure
Include	direction = External	direction = External	direction = External	direction = External
Exclude				
Group By				
Group By	Host Origin = 10.10.10.101	Host Origin = 10.10.10.101	Host Origin = 10.10.10.101	Host Origin = 10.10.10.101
Unique Value (Host Impacted)	Host Impacted = Server A	Host Impacted = Server B	Host Impacted = Server C	Host Impacted = Server X
Measurement (Occurrence)	Classification Log Count = 3			Log Count >= 10
Live Time (Time Limit)	Past 30 minutes			
Evaluation Frequency	Every 10 minutes			
Relationship Time				
N/A	Expression: Unique Value Host Impacted >= 3			Expression: Classification Log Count >= 10